SailPoint IdentityIQ

Version 8.1

Release Notes

This document and the information contained herein is SailPoint Confidential Information

Copyright and Trademark Notices.

Copyright © 2020 SailPoint Technologies, Inc. All Rights Reserved.

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

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

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

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

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

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

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

IdentityIQ Release Notes

These are the release notes for SailPoint IdentityIQ, Version 8.1

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 Feature Updates

IdentityIQ 8.1 provides new features and capabilities across the product, including Compliance Manager, Lifecycle Manager, the Governance Platform, and Connectivity. Key enhancements in the release include:

Feature Name

IdentityIQ Version 8.1 introduces the following new features or enhancements. For a more detailed description of the changes, see

Feature/Enhancement	Description
IdentityAI Recommendations Localized for German, French, Dutch, Spanish, and Italian.	You can now view your IdentityAI recommendations for access requests or certifications in these languages in addition to English.

Feature/Enhancement	Description
IdentityAI Automated Approvals for Certifications	With this feature activated, any access review item that has a recommendation of thumbs up, is automatically moved from the Open tab to the Review tab with a Decision of Approved. The icon for Auto Approved Recommendations is the standard thumbs up icon, with a star. Users will still have to review and sign off on these auto approved items in the Review tab. Users can undo the IdentityAI decision and move the item back to the Open tab for further review if needed. • AutoApproved information is captured in Reporting • A filter option is available to show all Auto Approved items
Configure what appears on Remove Access tab	Similar to how you can control what shows up in Add Access tab, you can now configure what entitlements and roles show up under the Remove Access tab. You can Sync these tabs to show the same information for both Add Access and Remove Access requests.
Edit Preferences page is now 508/WCAG Compliant	There are multiple tabs instead of a single page for General, Update Password, and Security Questions. If you are the system administrator, you will not have Security Questions. The Security Questions option must be enabled in the Login Configuration for it to appear for other users.
Support for Google Cloud Platform	Hosting IdentityIQ within Google Cloud's IaaS Platform, is now a supported option.
File Access Manager Integration	IdentityIQ is now very deeply integrated with File Access Manager for customers using the File Access Manager module. The integration supports a variety of use cases (detailed below) that bring the deep insights of File Access Manager to the business user, providing the context needed to make effective and efficient access decisions.
Support for Classifications	IdentityIQ now supports the concept of classifications on managed attributes. Classifications can be imported from File Access Manager, third party applications, or set manually within IdentityIQ. For example, in the context of IdentityIQ, when using File Access Manager classifications, IdentityIQ is displaying a business user's effective access to data that is granted through a role or entitlement.
Classifications available within Life Cycle Manager for access requests	Within Life Cycle Manager, you have the option to configure classifications to be displayed or hidden for access requests that are submitted. Review of submitted access requests on the approvals page will always display classifications if available.

Feature/Enhancement	Description
Classifications available within Certifications	When scheduling identity-based certifications, classification information can now be included as additional relevant data to assist Approvers making access review decisions. New filtering capabilities have also been added when scheduling certifications to support the creation of reviews focused on entitlements and roles that provide access to endpoints tagged with the selected classifications. When performing an access review containing classifications, Approvers will see a new icon on access items which have an associated classification and can hover on this icon to view additional details.
Classifications available within Advanced Policies	Several options have been added to extend the creation of Advanced Policy Rules. • Role and entitlement attributes can now be used to filter access in a policy • Match term operations for all advanced policy rules items have been extended to include `equals`, `not equal to`, and `null`. With these enhancements, policies have now been extended to support advanced use cases such as: • If user role = "Finance", then user cannot access data tagged with classification "PCI" • If user entitlement = "HR", then user cannot access `\\sample_directory\HR_group\`
Classifications available within Entitlement Catalog	Classification information is now displayed on affected items in the Entitlement Catalog. Additional filtering capabilities also allow the catalog to be filtered to entitlements that provide access to endpoints tagged with the selected classifications. Users will see a new icon on entitlements which have an associated classification and can hover on this icon to view additional details.
Classifications visible on Identity page	When viewing or editing the identity page, a new classification icon will display for any entitlements that have classifications assigned. Clicking on the classification icon will display more details.
Classifications available from Advanced Analytics	In the Advanced Analytics page, you can now search for roles and entitlements using classifications as search criteria.
Improvements to Role Details consistency across the application	Role Details dialogs have been enhanced to be consistent when accessed from anywhere within the application.
/Alerts SCIM API Endpoint	A standard SCIM API endpoint for /Alerts has been created to allow File Access Manager and third party applications to push alerts to the IdentityIQ Alerts framework for realtime processing. The endpoint allows for both creation of new alerts (POST operations) and checking of status of existing alerts (GET operations).
Data Governance Menu and Dashboard Widgets	Deep link capabilities have been add to File Access Manager from IdentityIQ to enable efficient navigation. In addition, two new widgets (Sensitive Data Exposure and Sensitive Resources Missing Owners) have been added to the IdentityIQ dashboard.

Feature/Enhancement	Description
Require Comments on Revoke Action for Certifications	A new configuration option, **Require Comments with Revocation**, in the Compliance Manager and Certification Scheduler user interfaces, now controls whether comments will be required for both item and account revocations, both single and bulk.
Connector Infrastructure	The AfterProvisioning Rule is now triggered post provisioning, even if the provisioning fails.
Application Reconfiguration	Application reconfiguration will now work for applications with no default schema, such as Delimited File, Web Services, JDBC. This enables the flexibility to select schema values and provisioning policies, even when a default value has not been set.

Connectors and Integration Modules Enhancements

New Connectors

IdentityIQ Version 8.1 delivers new, out-of-the-box connectors for the following enterprise applications, which simplifies the connectivity of these systems.

New Connectors	Description
S/4HANA Cloud	Net new Connector to support management of Business Users and Business Roles of SAP S/4HANA System.
Service Desk Integration Module	SailPoint transitions to new ServiceNow store-based listings for the cross-platform connector-based Service Desk integration.

Active Directory

Connector	Description	Benefit
Active Directory	Provides an option to control the number of partitions while configuring auto-partitioning.	Customer can now control the number of partitions created during partitioned aggregation to suit their environment.
	New Active Directory applications created will be optimized to avoid getting LDAP referrals during aggregations.	Enhanced to improve performance.
	Supports aggregating and provisioning of DialPlan attribute for a Microsoft Skype for Business User when defined under account schema.	During provisioning the DialPlan attribute can be set out of the box.

Amazon Web Services

Connector	Description	Benefit
Amazon Web Services	Upgraded the `aws-sdk-module.jar` as a few security vulnerabilities are addressed in the newer version.	Enhanced security for customer data.

Azure Active Directory

Connector	Description	Benefit
Azure Active Directory	Supports managing identities present in Azure Active Directory B2C.	Using Azure Active Directory Connector in B2C mode customers can now manage their consumer landscape from single point.
	Supports managing guest accounts in Azure Active Directory B2B collaboration mode.	Using Azure Active Directory Connector you can now manage your Guest users (B2B).
	Includes support for managing Office 365 groups.	Using Azure Active Directory Connector customers can now manage complete operations of Office 365 groups.
	Supports both the HTTP and HTTPS proxy configurations.	Connector can now communicate through a proxy server.

AIX, Linux and Solaris

Connector	Description	Benefit
AIX, Linux and Solaris	No longer use the Ganymed SSH-2 library. For enhancing the security, AIX, Linux and Solaris Connectors use `sshj-0.27.0.jar` file.	Enhanced to remove dependency on an outdated library to ensure business continuity.

Cerner

Connector	Description	Benefit
Cerner	Supports aggregation and provisioning for organization attribute.	With the introduction of organization as an attribute, administrators can now assign the exact organization that the user is entitled to, enabling better governance.
	Supports aggregation and provisioning of organizationGroup as a group object.	With the introduction of organizationGroup as a group schema attribute, administrators can assign the exact organization group that the user is entitled to, enabling better governance.
	Supports **replace** and **add** operations for username on the accounts.	Administrators will be able to directly add the username parameters from IdentityIQ for the record, achieving increased productivity.

Connector Gateway

Connector	Description	Benefit
Connector Gateway (Jan 2020)	For secure communication between components, TLS is recommended.	Supports TLS communication which ensures higher security.

Cloud Gateway

Connector	Description
Cloud Gateway	The IdentityIQ Cloud Gateway now bundles tomcat version 9.0.24.

Delimited File

Connector	Description	Benefit
Delimited File	No longer uses the Ganymed SSH-2 library. For enhancing the security, Delimited File Connector now uses `sshj-0.27.0.jar` file.	Enhanced to remove dependency on an outdated library to ensure business continuity.
	Supports SFTP file transport.	Connector now has the ability to connect to a SFTP server in addition to supporting FTP and SCP.

Epic Healthcare

Connector	Description	Benefit
Epic Healthcare	Supports different types of UserID, such as External, Internal, and SystemLogin.	Flexibility for the customer to select the UserID type.
	Supports SSL Client Certificate Authentication.	Better security as the connector supports two-way SSL (Mutual authentication) method.

G Suite (Google Apps)

Connector	Description	Benefit
G Suite	The default schema attributes in a newly created application are optimized for improved aggregation performance.	Modified default values to ensure better performance.

IBM DB2

Connector	Description	Benefit
IBM DB2	Supports TLS communication.	Enhanced security through TLS.

Mainframe Connectors

Connector	Description	Benefit
RACF, TopSecret and ACF2	DES/3DES encryption has been deprecated from IdentityIQ. For secure communication between components, TLS is recommended.	DES / 3DES encryption is obsolete and hence deprecated to safeguard customers data.

Microsoft SharePoint Online

Connector	Description	Benefit
Microsoft SharePoint Online	Supports fetching of Admin of Sites attribute during aggregation to provide visibility to administrators of site collections.	Using this attribute, you can now manage the access for Admin of sites.

Microsoft SQL Server

Connector	Description	Benefit
Microsoft SQL Server	Supports TLS communication.	Enhanced security through TLS.

Oracle NetSuite ERP

Connector	Description	Benefit
Oracle NetSuite ERP	Enhanced to work with Oracle NetSuite Web Service version WSDL_v2019_1_0	Support with latest version of WSDL of NetSuite ensures business continuity.
	Supports delete operation only when the isDeleteEnable attribute is enabled on the application object.	The default behavior of the connector is changed to ensure accounts are not deleted on a termination event.
	Application ID is now a mandatory parameter if the authentication type for the service account is set to **User Credentials**. Previously created application must provide a value for this parameter for the operations to work.	With the introduction of **Application ID**, the Connector ensures deeper governance by uniquely identifying users and organizations, thus ensuring better security for the customers data.
	Supports Token Based Authentication.	Token based authentication ensures enhanced security.

Okta

Connector	Description	Benefit
Okta	Supports aggregation and provisioning for multiple factors for users.	Additional security ensures secure access for the business users.
	Provides control on sendEmail parameter.	Better control on sending emails to users, thus keeping a check on organization privacy policies.
	Supports setting a recovery question and answer while provisioning an account in Okta native system.	Enabling users to create recovery question during account provisioning helps fewer IT support calls for lost/forgotten passwords.
	Supports a Credential Provider User, such as the Federation/Social Provider user in an Okta native system.	The connector now supports user creation from the Central Identity Stores, enabling enterprises to truly use the store as a golden source of user information.
	Improved aggregation performance by adding partitioned aggregation support.	Enhanced aggregation performance leading to lesser wait time to get the latest data for governance.

Oracle Fusion HCM

Connector	Description	Benefit
Oracle Fusion HCM	Supports delta aggregation.	Helpful for aggregating changed data and improved performance.
	Supports updating email and phone attributes.	Missing/incomplete user information can be updated through write-back mechanism.
	Supports provisioning and aggregating of custom attributes for person/employee.	Gives customers the flexibility to provision and aggregate custom attributes as per the organizations security policies.
	Supports aggregating active/inactive employees, contingent workers, pending workers and non-workers.	Ability to aggregate different types of records improves governance.
	Aggregates future hire and termination records based on the effective date offset.	Users can aggregate relevant data required for the business and thus better governance.

Oracle HRMS

Connector	Description	Benefit
Oracle HRMS	Supports the creation of employee records in Oracle HRMS.	Oracle E-Business Suite customers will now have the ability to manage the lifecycle of a user even when Oracle HRMS is not used as the authoritative source.

Oracle ERP – PeopleSoft

Connector	Description	Benefit
Oracle ERP – PeopleSoft	Enhanced user interface making it easer to read and understand.	Better user experience with enhancements in the user interface.
	Enhanced to use Application Libraries for configuring PeopleSoft specific jars instead of Jar Locations.	Standardizing the use of libraries ensures less maintenance.
	By using the zip file containing pre-configured PeopleSoft Component Interface Utility project, customers are no longer require to manually configure the component interface in the PeopleSoft Managed system.	The pre-configuration enables the customer to automatically have the Component Interface Utility configured in the PeopleSoft Managed system. This pre-configured package is agnostic to any version of PeopleTools supported by SailPoint.

PeopleSoft HCM Database

Connector	Description	Benefit
PeopleSoft HCM Database	Enhanced user interface making it easer to read and understand.	Better user experience with enhancements in the user interface.
	Enhanced to use Application Libraries for configuring PeopleSoft specific jars instead of Jar Locations.	Standardizing the use of libraries ensures less maintenance.

SAP HR/HCM

Connector	Description	Benefit
SAP HR/HCM	Support for Central Person ID and Person ID external streamlines the management of employees having multiple employments and global assignment records. Newly created applications will now have Person ID as the native identity.	The enhanced connector streamlines the management of employees having multiple employment and global assignments records.

SAP Governance Application Module - SAP GRC

Connector	Description	Benefit
SAP GRC	Enhanced to respect the sunrise and sunset dates while provisioning SAP Roles in IdentityIQ.	This enhancement makes granting of access using SAP Roles based on sunrise and sunset dates seamless thus improving user experience and improved governance.

Salesforce

Connector	Description	Benefit
Salesforce	Supports aggregation and provisioning of the Queue Names associated with an account.	This enhancement improves the overall access governance of an Saleforce account.

ServiceNow

Connector	Description	Benefit
ServiceNow	Supports ServiceNow Table API version V2.	Latest API's ensures better connector performance.

SuccessFactors

Connector	Description	Benefit
SuccessFactors	Supports aggregation of additional schema attributes without having to write any custom code.	Greater flexibility and better user experience.
	Supports provisioning for the BusinessPhone, PrimaryEmailAddress and Username attributes.	Connector now offers update of (write back) attributes out of the box. Additional rules are not required.

Sybase

Connector	Description	Benefit
Sybase	Supports TLS communication.	Enhanced security through TLS.

SQL Loader

Connector	Description	Benefit
SQL Loader	Connector enhanced to access data files placed on a FTP server.	This enhancement gives more flexibility and better user experience.

System for Cross-Domain Identity Management (SCIM) 2.0

Connector	Description	Benefit
System for Cross-Domain Identity Management 2.0	Supports partitioned aggregation based on SCIM 2.0 API filters.	Better aggregation performance.
	Connection Timeout parameter can now be configured from the user interface for the SCIM 2.0 Connector.	Connection Timeout parameter helps customers to set timeout values through user interface for a better user experience.

Web Services

Connector	Description	Benefit
Web Services	Enhanced to support OAuth2.0 Password Grant Type as a way to get access token.	Better security and flexibility.

Workday

Connector	Description	Benefit
Workday	Supports filtering using eligibility criteria.	Eligibility criteria provides endless possibilities for applying filters in aggregation of workers records. Using this calculative field customer can now select what needs to be aggregated.
	Supports aggregation of multi-valued attributes.	Connector is enhanced to handle attributes containing multiple value during aggregation without having to write any additional code thus improving user experience.
	Supports Home Contact Change and Work Contact Change API's.	Connector now supports latest API mechanism for updating attributes.

Workday Accounts

Connector	Description	Benefit
Workday Accounts	Supports provisioning Roles to Workday accounts.	Adding access management into workday accounts, through which customer can manage the complete access management for Workday Accounts driven by Roles.
	Supports fetching the organization roles of workers.	Adding access management into workday accounts, through which customer can manage the complete access management for Workday Accounts driven by Roles.

Read-only Connectors (UNIX and XML)

Connector	Description	Benefit
UNIX and XML	No longer use the Ganymed SSH-2 library. For enhancing the security, UNIX and XML Connectors now use `sshj-0.27.0.jar` file.	Enhanced to remove dependency on an outdated library to ensure business continuity.

Connectivity Platform and Language Updates

Connector/Component	New Platform Version
Active Directory	Active Directory Connector now supports Microsoft Skype for Business Server 2019.
Cloud Gateway	The Cloud Gateway is now supported on the following operating systems: • Red Hat Enterprise Linux 8.0, 7.6 and 7.4 • Windows Server 2016
IBM i	The IBM i Connector now supports version IBM i 7.4.
Lotus Domino	Lotus Domino Connector now supports IBM Lotus Domino version 10.0.1.
Linux	Linux Connector now supports the following versions: • Red Hat Enterprise Linux version 8.1 and 8.0 • SUSE Linux Enterprise Server version 15 • Ubuntu version 18.04 LTS
Microsoft SQL Server	The Microsoft SQL Server Connector now supports Microsoft SQL Server 2019.
Oracle ERP - PeopleSoft	PeopleSoft Connector now supports PeopleSoft Tools version 8.57.
Oracle	Oracle Database Connector now supports Oracle Database 18c.
Oracle E-Business Suite	Oracle E-Business Suite now supports Oracle E-Business Suite version 12.2.7 and 12.2.8.
PeopleSoft HCM	PeopleSoft HCM Database Connector now supports PeopleSoft Tools version 8.57
ServiceNow	The Identity Governance Connector for ServiceNow now supports the following ServiceNow releases: • Orlando • New York
Service Desk	The IdentityIQ for Service Desk Integration Module now supports the following ServiceNow releases: • Orlando • New York
SAP ERP - SAP Governance Module	The SAP Connector is now certified with SAP Supply Chain Management (SCM) and SAP Advanced Planning and Optimization (SAP APO)

Connector/Component	New Platform Version
Workday	The Workday connector now supports Workday API version 32.1

Connectivity Dropped Platform Support

Connector/Integration Module	Dropped Platforms
IBM i	The IBM i Connector no longer supports IBM i version 7.1
Connectors	SailPoint announces the end of support for Windows Server 2008 and Windows Server 2008 R2 for connectivity as extended support for Windows Server 2008 and 2008 R2 has been ended by Microsoft
ServiceNow	The Identity Governance Connector for ServiceNow no longer supports the Kingston ServiceNow release.

Dropped/Deprecated Connector Support

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

- Microsoft Project Server

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

- MobileIron Enterprise Mobility Management
- Good Technology Enterprise Mobility Management
- ServiceNow Service Catalog API Integration
- ServiceNow Service Catalog Integration
- ServiceNow Service Desk Integration (IntegrationConfig based module)

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

Important Upgrade Considerations

IdentityIQ Version 8.1 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.

- Aspectj 1.9.4
- Bouncycastle 1.64
- Apache Commons BeanUtils 1.9.4
- Apache Commons Codec 1.13
- Guava 26
- HXTT Text
- Jackson 2.10
- Jersey Test Framework 2.29
- Jersey 2.29
- JSF 2.20
- log4j 2.11.1
- Lucene 8.2
- Netsuite
- ojdbc 8
- Opensaml 3
- p6spy
- Primefaces 7
- sshj 0.27
- TestNG 7.1
- Twilio 7.37.2
- Xmlunit 1.6

MySQL Restart

Due to library and driver upgrades, it might be necessary to restart MySQL after upgrading to IdentityIQ version 8.1 if errors are encountered after the upgrade.

REST Endpoints Removed

The following 2 REST endpoint have been removed as a part of this release:

- /ui/rest/requestAccess/accessItems/{itemid}/simpleEntitlements
- /ui/rest/requestAccess/accessItems/{itemid}

Oracle ojdbc8 driver

If you are using the Oracle ojdbc8 driver you should make a configuration change to the JVM parameters. Disable `nio` by adding `-Doracle.jdbc.javaNetNio=false`. This prevents issues where the database connection is closed in error

Websphere Shared Libraries

Shared libraries for Websphere have changed. See Advanced Installation Information - Deploy Using Websphere in the *IdentityIQ Installation Guide* for more details.

getObject Method Deprecation

In 8.1 the getObject method has been deprecated and will be removed in a future release. All uses within IdentityIQ have been replaced with deterministic methods getObjectById or getObjectByName. If you have any custom code or rules using getObject, you should replace it with one of the deterministic methods above.

Impact Analysis

Impact Analysis, triggered in a workflow using the launchImpactAnalysis action, will now take two new arguments to control the analysis. The argument doRoleAssignment will enable autoAssignable roles to be included in the Identity gains/loss metrics. The argument maxGainLoss will enable configuring the maximum number of Identity names included in the gains/loss list of Impact Analysis (previously set to a maximum of 100). As a result, the Impact Analysis result in the user interface will now show all of the Identities configured. Since these values can affect how Impact Analysis will scale, appropriate test efforts with reasonable values is recommended.

Reference Certification Definitions By Name

During upgrade we will examine certification schedules to ensure they are referencing certification definitions by name. If you have any artifacts of this type that are imported into IdentityIQ, you need to make sure they are referencing name as well.

Full Text Index

Full text indexes need to be recreated after upgrade due to Lucene update.

WebLogic 12.2.1.2

WebLogic 12.2.1.2 presents a NoSuchMethodError after logging into IdentityIQ 8.1. This was due to a bug addressed in WebLogic 12.2.1.3. We recommend you upgrade to at least WebLogic 12.2.1.3.

JDBC Driver for MySQL

The JDBC driver for MySQL has been upgraded in this release. If you choose to use the driver shipped with IdentityIQ, you will receive a warning regarding deprecated class **com.mysql.jdbc.Driver**. To prevent this, any references to `com.mysql.jdbc.Driver` should be updated to use the new class of `com.mysql.cj.jdbc.Driver`.

Tomcat Versions 8.5.49 and 9.0.29

Tomcat versions 8.5.49 and 9.0.29 fail to load the IdentityIQ login page and throw a StackOverflowError. Later versions of Tomcat, 8.5.50 and 9.0.30 do not present this error.

Oracle HRMS

With this release of IdentityIQ 8.1, the Oracle HRMS Connector supports the creation of employee records in Oracle HRMS. SailPoint does not recommend creation of records into HRMS through automated process.

SailPoint recommends to use the automated process of creating employee records in Oracle HRMS feature from an efficiency perspective. This feature has been introduced to automate user creation into Oracle HRMS only when Oracle HRMS is not the authoritative source for user information. Oracle E-Business Suite only accepts Person ID from its HRMS systems. This feature helps provide access to employees to Oracle E-Business Suite modules based on appropriate permissions. The feature also supports employee termination/separation once the trigger has been received from the authoritative source. Aggregation performance has been improved in this release.

Active Directory and LDAP (ADAM)

With this release of IdentityIQ 8.1, the Active Directory/LDAP (ADAM) Connector have been certified for all supported functionalities with LDAP channel binding and LDAP signing enabled on domain controller (Microsoft Advisory **ADV190023**) and works as expected over secure channel using TLS\SASL protocol.

Oracle NetSuite

With this release of IdentityIQ 8.1, the introduction of **Application ID** in Oracle NetSuite Connector, ensures deeper governance by uniquely identifying users and organizations. **Application ID** is now a mandatory parameter if the authentication type for the service account is set to **User Credentials**. Previously created application must provide a value for this parameter for the operations to work.

TaskSchedule Upgrader

TaskSchedule upgrader will upgrade the executor from id to name along with the existing upgrader logic to convert certificationDefinitionId from id to name.

Request Access Deep Links

If you are using deep links for Request Access, you need to include the quicklink name in your query parameters in order to ensure that the details dialogs work properly.

OAuth Support

IdentityIQ now supports OAuth on all REST endpoints within IdentityIQ, including the Plugin Framework.

Supported Platforms

Operating Systems

Note: Linux Support: The distributions and versions of Linux 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.

- IBM AIX 7.1 and 7.2
- Red Hat Linux (RHEL) 8.0 and 7.7
- Oracle Linux (using RHE Kernel Mode) 8.1 and 8.0
- SUSE Linux 15 and 12.4
- Windows Server 2016 and 2019
- Solaris 10 and 11
- CentOS 8.0 and 7.7

Application Servers

- Apache Tomcat 9.0 and 8.5
- Oracle WebLogic 12.2.1.3 or greater
- IBM WebSphere 9.0
- JBoss EAP 7.2
- IBM WebSphere Liberty 19.0.0.5

Databases

- IBM DB2 11.5 and 11.1
- MySQL 5.7 and 8.0
- MS SQL Server 2019, 2017, and 2016
- Oracle 19c, 18c
- AWS Aurora
- Azure SQL

Java Platform

- Oracle JDK 8 and 11
- AdoptOpenJDK 8 and 11 for Windows
- Red Hat OpenJDK 8 and 11 for Linux

Browsers

- Google Chrome Latest Version
- Internet Explorer 11 and Edge

- Safari 12
- Firefox Latest Version

Mobile User Interface OS/Browser Support

- Android 10
- iOS 13 with Safari

Cloud Support

- AWS EC2
- AWS Aurora
- AWS RDS
- Azure VM
- Azure Azure SQL
- Google Cloud Platform Google Compute Engine

Languages

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

Resolved Issues

CONBOGIBEE-1004	The Windows Local Connector now uses the Fully Qualified Domain Name (FQDN) of the target Windows host instead of the NetBIOS name while connecting to it.

CONBOGIBEE-1102	Azure Active Directory Connector is more resilient in case of authorization failures due to expiration of access token while aggregating large set of data.
CONBOGIBEE-1249	Azure Active Directory Connector now supports retry using Retry-After value returned by API.
CONCHENAB-2765	Workday Connector now aggregates the most recent record of a worker with multiple termination records.
CONCHENAB-2979	Workday Connector no longer fails on WebSphere application server.
CONNCHENAB-3000	Workday Connector now handles rescinded and corrected worker events from the Workday system.
CONCHENAB-3055	Cloud Gateway keystore password decryption no longer fails after upgrade.
CONCHENAB-3060	The Salesforce Connector now fetches the query result in chunks while fetching entitlements to avoid query timeouts. The PublicGroup and PermissionSet can be skipped from account aggregation by deleting them from the schema.
CONCHENAB-3076	Workday Connector now populates FUTURE_ACTION**,** FUTURE_DATE, and LAST_DAY_OF_WORK attributes for an employee worker when the last day of work is before the termination date.
CONCHENAB-3196	The Workday Connector parallel aggregation now works with a smaller chunk size.
CONCHENAB-3218	Workday Connector now provides an option to fetch reference descriptors in the responses from Workday.
CONCHENAB-3266	IdentityIQ Cloud Gateway Synchronization Task will now fail if the keystore is not valid in the Cloud Gateway.
CONCHENAB-3291	Errors during provisioning operations will now correctly appear in the user interface if an application is using the Cloud Gateway as a proxy.
CONCHENAB-3318	System for Cross-Domain Identity Management 2.0 Connector would update the null string values with a null object in the JSON request body of the PUT request.
CONCHENAB-3330	System for Cross-Domain Identity Management 2.0 Connector now regenerates access token once expired.
CONCHENAB-3352	System for Cross-Domain Identity Management 2.0 Connector now excludes read-only attributes from JSON body in case of PUT request.
CONCHENAB-3463	The ITIM Application Creator task for IBM Security Identity Manager Integration Module no longer fails with the following error: `not an ITIM application`
CONCHENAB-3471	The Workday Connector now escapes the HTML characters in password.
CONCHENAB-3505	AirWatch Enterprise Mobility Management Connector now does not fail intermittently due to missing **Accept** header.
CONETN-2358	The G Suite Connector no longer causes ConnectorException when running delta aggregation to fetch users from external domains.
CONETN-2485	The SAP ERP - SAP Governance Module Connector no longer fails when provisioning a Contractual User Type ID using the same language as it was aggregated.
CONETN-2564	The LDAP Connector now considers the Group Member Search Filter configuration when provisioning entitlements for an account.

CONETN-2598	The Active Directory Connector aggregates all accounts even when a communication exception occurs.
CONETN-2599	The Microsoft SQL Server Connector no longer fails on provisioning operations for case sensitive database.
CONETN-2620	The Oracle E-Business Suite Connector no longer closes the connection when more than one provisioning operations are performed in a single account request.
CONETN-2622	In Active Directory Connector, when a Disable provisioning request is received and if the RegistrarPool attribute is empty or null, the account would be disabled in Active Directory and the Skype account would be deleted.
CONETN-2623	The Microsoft SharePoint Server Connector now persists the ParentWeb attribute for a group and displays it as a Managed Attribute for the group.
CONETN-2633	Password reset for a serverless Active Directory application will reset the password successfully when enforcedPasswordPolicy is set to `true`.
CONETN-2644	The IQService will log INFO level debug messages when the trace level is set to 2.
CONETN-2656	The Oracle Database Connector now correctly synchronizes the user quota to native database.
CONETN-2658	The Workday Connector now supports http and https based proxy servers.
CONETN-2666	In JDBC Connector the **Test Connection** would no longer be successful when a wrong user password is provided.
CONETN-2677	The LDAP Connector no longer skips nativeObjectType schema attribute when provisioning a new account with objectClass attribute.
CONETN-2682	The G Suite Connector no longer deletes custom entitlements for an account when running PIRM task with isSkipAlias set to `true` in the application configuration.
CONETN-2689	The Microsoft SharePoint Server Connector no longer deletes an account from a Site collection when a group without permissions is revoked.
CONETN-2696	The G Suite Connector no longer attempts retry logic unnecessarily during Group Aggregation when the following message is received: `HTTP response code 200 (OK)`
CONETN-2703	During group aggregation, the PeopleSoft Connector no longer fails when getIds method is not found in Component Interface.
CONETN-2718	During delta aggregation, the Workday Connector no longer updates the future-dated attributes before actual effective date.
CONETN-2722	The Active Directory Connector now displays Octet String and SID type attributes in correct format.
CONETN-2743	The Active Directory Connector now correctly aggregates the delta from child domain or sub-OU when running delta account aggregation or delta account-group aggregation with iterate search filter in place.
CONETN-2748	The PeopleSoft Connector no longer causes `NullPointerException` when a user password is reset along with an attribute synchronization.

CONETN-2751	During provisioning operation, the Active Directory Connector no longer fails with the following error for move/rename operation: `Object reference`
CONETN-2773	The Workday Connector now supports retrieving the MANAGER_ID attribute for a worker regardless of the manager's worker type.
CONETN-2778	The Active Directory Connector now supports the timeZone attribute used to define the timeZone with which customer wants to provision or view accountExpires attribute. This attribute can be used if customer wants to change the default behavior of provisioning and displaying of accountExpires attribute. This attribute accepts value in string format with the following valid values: • **epoch**: to provision and view accountExpires attribute in Active Directory epoch format. • **Continent/City**: this format is similar to standard format which Java supports. For example, if customer wants to provision and view accountExpires attribute in Indian Standard Time then timeZone in application must be set as Asia/Kolkata.
CONETN-2808	The Active Directory Connector no longer displays the `NullPointerException` when nativeIdentity in provisioning plan is null or empty.
CONETN-2826	The provisioning request for Active Directory Connector now no longer fails with the same error when the setAttributeLevelResult attribute is set to `true`.
CONETN-2857	The memberAttribute of group schema for multi-group application with object type as group would be updated only once after upgrading the application and will no longer be modified when application is saved through user interface. The memberAttribute can be modified as required thereafter.
CONETN-2858	During delta aggregation, the Workday Connector no longer fails for future terminating accounts when using Organization_Reference_ID attribute.
CONETN-2872	During aggregation, the Azure Active Directory Connector would no longer take more time for completion. Earlier there was an impact on aggregation performance after the proxy support was introduced.
CONETN-2874	The SAP HR/HCM Connector now correctly aggregates STAT2_Current attribute when service account does not have authorization for all Infotype Subtypes.
CONETN-2895	The ADAM LDAP Connector now considers Group Member Search DN attribute of application in account aggregation.
CONHELIX-1208	The EPIC Connector now uses appropriate headers to connect to EPIC 2019.
CONHELIX-1622	The Delimited File Connector's FTP file transport mode would now no longer fail due to Buffer size.
CONHOWRAH-2011	For the Active Directory Connector, the accountExpires attribute now displays the date and time in the following format: `MM/dd/yyyy hh:mm:ss a z` For example, **01/01/2020 12:00:00 AM IST**
CONHOWRAH-2209	The Active Directory Connector has been certified against Microsoft advisory **ADV190023** and all connector functionalities works fine when LDAP channel Binding and LDAP Signing configuration are enabled on Domain Controller.

CONHOWRAH-2224	SailPoint recommends use of TLS configuration to secure communication between IdentityIQ and IQService. The IQService Key Exchange task is now deprecated.
CONJUBILEE-99	The Web Services Connector now supports the provisioning plan as an additional parameter in the WebServiceBeforeOperationRule.
CONJUBILEE-192	The Web Services Connector is now able to replace plans identity attribute in the relative URL or payload.
CONJUBILEE-205	The Web Services Connector now correctly replaces the native identity placeholder for create operation.
CONJUBILEE-218	The Web Services Connector now displays a warning in the logs instead of an error when regenerating an access token.
CONJUBILEE-226	The Web Services Connector now supports a JSON array as a top element in HTTP requests.
CONJUBILEE-245	The Web Services Connector now supports replacement of application attributes in OAuth2 token URL.
CONJUBILEE-247	The Salesforce Connector can now provision multiple accounts in Salesforce in single request.
CONJUBILEE-286	The Salesforce Connector now provides a user-friendly error message when disabling users that have a custom attribute with hierarchy data type disabled in Salesforce.
CONJUBILEE-296	The Web Services Connector now correctly handles the $ character in a URL.
CONJUBILEE-307	The SCIM 2.0 Connector now skips the extra redundant group update call while creating account with entitlement.
CONJUBILEE-308	The Salesforce Connector now supports disabling account along with entitlement removal.
CONJUBILEE-317	The Web Services Connector is now able to provision entitlement with boolean values.
CONJUBILEE-318	The Web Services Connector now bypasses the proxy for hosts mentioned in nonProxyHosts list.
CONJUBILEE-319	The Web Services Connector now supports cookies for HTTP requests.
CONJUBILEE-320	The **Test Connection** performance for Salesforce Connector is now optimized.
CONJUBILEE-334	During aggregation, the Web Services Connector now updates the access token generated during execution of second endpoint.
CONJUBILEE-341	Cloud Gateway now parses permission object correctly.
CONJUBILEE-348	The Web Services Connector now supports exceptions to be displayed from WebServiceAfterOperationRule for all operations.
CONJUBILEE-349	The Web Services Connector now validates OAuth2 access token and generates a new token, if required, before sending requests to API endpoints.
CONJUBILEE-394	When paging is configured, the Web Services Connector now parses the JSON response correctly.
CONMF-480	Mainframe Connectors now handle various field delimiters while processing revoke target permission requests.
CONMF-531	Mainframe Connectors no longer log informational messages as ERROR in log file.

CONNAMDANG-1743	During aggregation, the Sybase Connector now displays error messages for certain incorrect situations where continuing aggregation was irrelevant.
CONNAMDANG-1959	The Oracle NetSuite Connector can now create accounts by adding roles.
CONNAMDANG-2149	The Oracle NetSuite Connector now supports dynamic discovery of NetSuite system URL's.
CONNAMDANG-2376	The Oracle NetSuite Connector is now enhanced to set account employee status correctly.
CONPAMBAN-1816	The RSA Authentication Manager Connector now correctly aggregates all the accounts when Active Directory is configured as the identity source.
CONPAMBAN-1995	The RSA Authentication Manager Connector now handles large number of groups during the group aggregation.
CONPAMBAN-2050	Endpoint identification algorithms have been enabled by default in JAVA from version 8u181. Endpoint identification algorithms can be disabled by enabling disableLDAPHostnameVerification parameter in LDAP or Active Directory application. When parameter is enabled on any application it sets JVM property to disable Endpoint identification algorithms and the change applies to all LDAP connectors.
CONSEALINK-1118	The ServiceNow Connector now supports setting non-English characters for the email address field.
CONSEALINK-1175	The ServiceNow Connector supports TLS version 1.2 while connecting to the ServiceNow instance.
CONUMSHIAN-3146	The SuccessFactors Connector no longer fails when the token expires during aggregation and provisioning operations.
IIQCB-2426	Corrected issues with localization tokens for items in capabilities assigned by workgroups in the user rights tab of the identity warehouse.
IIQCB-2465	Application object attributes considered bottom-level (keys where the value is another map, or array containing maps) like domainSettings.password are now encrypted during import and save. Encryption is controlled by the encrypted attribute on the application and can contain MapUtil syntax to reference bottom-level attributes. Importing Active Directory - Direct applications that were exported from previous versions of IdentityIQ will not contain the encrypted attribute and should manually add the attribute before importing.
IIQCB-2513	Sunrise/Sunset Request object names now use the message catalog.
IIQCB-2514	Request object names created with a date will now have that date update when it changes.
IIQCB-2525	Privileged Access Management based Manager Approvals now properly redirect when the global forceClassicApprovalUI setting is set to true.
IIQCB-2527	The WebService application configuration page will now render correctly in Italian.
IIQCB-2529	To support accessibility, Aria labels are now applied to the **Find Users' Access** field and drop-down menu in the Manage User Access section of the Lifecycle Manager.
IIQCB-2530	For accessibility when navigating among tables in IdentityIQ using the T hotkey, table captions have been added to various data tables throughout the product.
IIQCB-2554	The request type drop-down will now have a paging toolbar enabling users to scroll through the remaining types that were previously hidden.
IIQCB-2560	[SECURITY] HttpSession is invalidated and creates a new session before login when single sign on methods of authentication are used.

IIQCB-2568	Corrected case where disable delegation forwarding was not actually disabling the ability to forward a WorkItem.
IIQCB-2571	Focus will now stay on the top-level menu option when the quicklink menu icon is selected.
IIQCB-2572	All selections in Advanced Analytics should now clear when **Clear Search** is clicked.
IIQCB-2586	Removed the outbox forwarding configuration option as that feature has been deprecated.
IIQCB-2588	When attempting to reset the password for other users, the **Submit** button is grayed out to prevent double clicks.
IIQCB-2590	When a user enters text that returns no results in a drop-down, **No results found** message is returned.
IIQCB-2613	The java classes sailpoint.connector.sm.SMInterceptor, sailpoint.connector.AbstractLogicalConnector, DefaultLogicalConnector, LogicalConnector and RuleLogicalConnector have moved from the connector-bundle.jar archive to the identityiq.jar archive.
IIQCB-2645	Provisioning can now more gracefully complete in situations where the ProvisioningResult has failed, but has no errors stored with it, which could also prevent the last refresh date on an identity from being updated.
IIQCB-2688	Added safeguards to prevent state which caused errors to be repressed in the user interface if multiple errors were thrown on the password reset page.
IIQCB-2735	The Manage User Access business process comment and assignment note dialog on the request item now have an accessible name.
IIQCB-2736	Date filter placeholder text now uses aria-label.
IIQCB-2740	The public API ComplexValue.containsAttributes() returns the correct boolean value indicating sub-attributes exist.
IIQETN-2472	Entitlements involved in a user's assigned attributes (done when an LCM request is made to provision an entitlement to a user) will no longer be replaced by roles. This will enable those users with assigned attributes to have their entitlement(s) removed by the same LCM actions without having to deactivate or remove the containing role.
IIQETN-2811	Require comments on revoke action feature has been added.
IIQHH-1021	The ToDo plugin has been updated on compass.
IIQHH-1162	The IdentityIQ Twilio integration is now using version 7 of the Twilio Java SDK.
IIQHH-1170	Duplicate EntitlementGroup values will no longer appear in an identity's XML after refresh.
IIQHH-1195	Apache Tomcat 8.5 has improved its support for Java 9+. The later versions of Apache Tomcat 8.5 have improved compatibility with Java 9+ than earlier versions of Apache Tomcat 8.5. If you are running with Java 11, yet are required to use Apache Tomcat 8.5 instead of Apache Tomcat 9.0, the later versions of 8.5 will be more robust and show fewer Java-related warnings.
IIQHH-1201	When exporting advanced analytics reports the **%** complete field should no longer exceed 100%.
IIQHH-1206	All Rest API endpoints and plugins support OAuth for authorization.

IIQHH-1225	Application schemas now have a descriptionAttribute attribute. It is used during group aggregation to indicate which of the group's attributes should be used to populate its corresponding ManagedAttribute's description.
IIQHH-1260	Using the advanced filter editor when creating or editing a role will now properly detect and use the desired boolean operator.
IIQHH-1370	In Advanced Analytics, viewing unmatched identities in the entitlements popup will now only show identities who do not have the selected entitlement.
IIQHH-1530	The field maxActive in JdbcUtil is now deprecated and will be removed in a future version. The maxTotal property should be used instead.
IIQHH-1606	It might be necessary to restart MySQL after upgrading to IdentityIQ version 8.1.
IIQHH-967	Privileged Access Management applications no longer require nativeIdentitier and source attributes for account and group schemas.
IIQKAP-371	Customers using the Oracle ojdbc8 driver should make a configuration change to their JVM parameters. Disable nio by adding `-Doracle.jdbc.javaNetNio=false`. This prevents issues where the database connection is closed in error
IIQKAP-493	Updated the list of certification configuration options in the user guide.
IIQKAP-510	[SECURITY] Shared libraries for websphere have changed. Please see Advanced Installation Information - Deploy Using Websphere, in the *IdentityIQ Installation Guide* for more details.
IIQKAP-526	Information on self certification options has been updated in the product documentation and in the Self-Certification in IdentityIQ documentation on compass.
IIQMAG-2218	The Privileged Access Management Module now supports aggregation of empty containers. The option **Include empty targets** has been added to the Target Aggregation task and, when enabled, empty targets are saved. (Option was added in IIQHH-1257)
IIQMAG-2389	The search bar on the Privileged Access Management page has been moved to be consistent with the location of the search bar on other pages.
IIQMAG-2392	To support accessibility, hotkeys, Page Up/Down and arrow navigation now work more predictably in the calendar control used throughout IdentityIQ.
IIQMAG-2394	Full text searching in the Manage User Access feature of Lifecycle Manager has been revised to return only results for items that are designated requestable.
IIQMAG-2396	The table on the entitlements tab in the Identity Warehouse now adjusts appropriately after a column in the table is resized.
IIQMAG-2407	The **Enable Help Windows** button in the Edit Preferences dialog has been removed, as it no longer applies to any portions of the user interface.
IIQMAG-2419	[SECURITY] As part of the rewrite of the Edit Preferences dialog, when SSO is enabled, the Password tab of the Edit Preferences dialog is not displayed, as users cannot change their passwords through this option with SSO enabled.
IIQMAG-2420	As part of the rewrite of the Edit Preferences dialog, a system configuration option was introduced to control the ability to change passwords through the IdentityIQ user interface. This option is located in **Gear Menu->Global Settings->Misc->Enable Change Password**. This setting is enabled by default.

IIQMAG-2504	In batch requests, a RemoveRole operation will correctly set negative=true on the RoleAssignment. This brings its behavior in line with removing a role normally using LCM Access Request. This setting is used to prevent roles with assignment rules that are revoked in a certification from being automatically reassigned after an identity refresh.
IIQMAG-2505	[SECURITY] Unsupported file types are now prevented from downloading from the file attachment overlay. Unsupported file types have always been blocked from being stored in the attachments database.
IIQMAG-2597	The Role Details dialog that is launched from LCM Access Requests and Approvals, Certifications, the Role Editor, and the Roles tab on the Identity Warehouse has been enhanced and standardized to provide more information about the role, its entitlements, and its hierarchy.
IIQMAG-2706	The following REST endpoint have been removed as a part of this release: • /ui/rest/requestAccess/accessItems/{itemid}/simpleEntitlements • /ui/rest/requestAccess/accessItems/{itemid}
IIQMAG-2815	Identity Administrators can no longer get into a state where they will not be able to save edits to an identity in the identity warehouse.
IIQMAG-2819	For access requests initiated from the Direct Reports widget on the home page, clicking **Details** for roles or entitlements will launch an empty dialog. If you need to examine role or entitlement details, launch the access request from the Manage Access quicklink.
IIQPB-882	In 8.1 the getObject method has been deprecated and will be removed in a future release. All uses within IdentityIQ have been replaced with deterministic methods getObjectById or getObjectByName. If you have any custom code or rules using getObject, you should replace it with one of the deterministic methods above.
IIQPB-897	Impact Analysis, triggered in a workflow using the launchImpactAnalysis action, will now take two new arguments to control whether assigned roles are processed and the number of identities to display in the gains/loss list of Impact Analysis
IIQPB-900	Corrected an issue causing Account Group aggregation to fail while trying to remove an account group with targetAssociations.
IIQPB-903	During upgrade certification schedules are reviewed to ensure they are referencing certification definitions by name. If you have any artifacts of this type that are imported into IdentityIQ, you need to make sure they are referencing name as well.
IIQPB-909	Negative assignment is no longer set when removing a manually assigned role. It is only set when removing roles assigned by rule.
IIQPB-910	Assignment detection will no longer happen for negative assignments during role detection.
IIQPB-913	Changing the account lockout criteria in login config will now log more detail if auditing is enabled.
IIQPB-921	When using WebSphere you must copy the `jakarta.ws.rs-api-2.1.6.jar` file to the shared library and add that jar name to the shared library list if you wish to use the File Access Manager or IdentityAI product integrations.
IIQPB-928	Fixed an issue with how the CorrelationModel is handled during Identity Refresh. This will prevent unexpected provisioning outcomes if an encountered role is not in the model.
IIQPB-929	Role Propagation will no longer remove entitlements required by other assignments.

IIQPB-941	On the Access Request list page, **Waiting on <approver>** is now displayed for each item in the request with an open approval.
IIQPB-942	Addressed a case where rejections from split provisioning might not be properly handled.
IIQSAW-1977	Changes were made to the identity selectors for certain features. Customers who are customizing the delegation or reassignment selects in certifications should verify that they are still behaving as desired. The context might have changed.
IIQSAW-2131	Identity Refresh no longer throws a ConcurrentModificationException when a combination of circumstances cause thread contention in the task.
IIQSAW-2151	WADL can now be generated successfully for all REST applications.
IIQSAW-2156	Target aggregation progress reporting now accurately reports the name of the target being processed.
IIQSAW-2160	Roles that have been revoked no longer appear in role membership certifications.
IIQSAW-2164	[SECURITY] The Jquery library was updated to version 3.4.1 across all pages.
IIQSAW-2165	[SECURITY] All list result REST resources and data source endpoints should be passed a limit parameter to limit results. If none is passed, the limit will default to 25 results. A maximum of 100 results is permitted.
IIQSAW-2166	Password/Question form fields now correctly update after a language change.
IIQSAW-2167	DEPRECATION WARNING: The automatic redirect from outdated certification URLs to current ones will be removed in the next version of IdentityIQ. Please verify any URLs in certification related email templates are pointed to valid current URLs.
IIQSAW-2174	Certain non-alpha-numeric characters, including "$;~<", in identity names no longer cause identities to be excluded when creating advanced identity certifications.
IIQSAW-2186	A new configuration option, **Require Comments with Revocation**, in the Compliance Manager and Certification Scheduler user interfaces, now controls whether comments will be required for both item and account revokes, both single and bulk. The requireAccountRevokeComments setting in xml configuration will no longer be consulted.
IIQSAW-2189	HTML elements in Group descriptions are now stripped out and no longer cause an exception during attempts to display them in the user interface.
IIQSAW-2193	For policy violations with multiple mitigations, the mitigation on the policy violation now expires on the expiration date of the most recently created mitigation.
IIQSAW-2206	Account decisions in Application Owner certifications are now maintained when editing decision.
IIQSAW-2212	Full text indices need to be recreated after an upgrade due to a Lucene update.
IIQSAW-2247	Targeted certifications can now be successfully generated when archiving excluded entities.
IIQSAW-2251	An access revocation action from a certification that generates a manual work item for the revocation no longer triggers native change detection.
IIQSAW-2256	Targeted certification entitlement filtering is now case insensitive on value.
IIQSAW-2323	Role details can now be viewed in access review for a renamed role.
IIQSAW-2360	When the skipLocalization flag is set to true in the ReportColumnConfigs it will skip localization when it is exported using LiveReport.

IIQSAW-2362	All pages now render correctly in Internet Explorer 11 compatibility mode.
IIQSAW-2389	A new configuration option provides the ability to disable localization of specific report columns. A skipLocalization attribute has been added to the <ReportColumnConfig> object.
IIQSAW-2447	[SECURITY] Deprecrated `com.mysql.jdbc.Driver`
IIQSAW-2472	[SECURITY] The sailpoint.tools.Util.convertToLowerUnderscore method have been removed due to security concerns with the gdata-appsforyourdomain library the method depends on.
IIQSAW-2474	WebLogic 12.2.1.2 presents a NoSuchMethodError after logging into IdentityIQ 8.1. This was due to a bug addressed in WebLogic 12.2.1.3. We recommend you upgrade to at least WebLogic 12.2.1.3.
IIQSAW-2476	[SECURITY] Deprecrated babel-runtime@6.26.0/lodash@4.17.4
IIQSAW-2479	[SECURITY] Error messages from REST calls are now HTML encoded in warning dialog.
IIQSAW- 2484	[SECURITY] Deprecrated `ojdbc6.jar`
IIQSAW-2502	[SECURITY] A user can no longer gain elevated access when the Lifecycle Manager Create Identity flow allows the requester or approver to define or modify the identity name.
IIQSAW-2507	The JDBC driver for MySQL has been upgraded in this release. If you choose to use the driver shipped with IdentityIQ, you will receive a warning regarding deprecated class com.mysql.jdbc.Driver. To prevent this, any references to com.mysql.jdbc.Driver should be updated to use the new class of com.mysql.cj.jdbc.Driver.
IIQSAW-2508	Periodic certifications are no longer updated to remove identities when the identity's status changes to inactive and the certification was configured to **Exclude identities marked inactive**.
IIQSAW-2555	[SECURITY] Certification names are now encoded to avoid cross-site scripting attacks during certification management.
IIQSAW-2562	Tomcat versions 8.5.49 and 9.0.29 fail to load the IdentityIQ login page and throw a StackOverflowError. Later versions of Tomcat, 8.5.50 and 9.0.30 do not present this error.
IIQSAW-2581	[SECURITY] A user can no longer gain elevated access when interacting with work items and archived work items in the Lifecycle Manager.
IIQSAW-2630	[SECURITY] Suggest filter functionality has been enhanced to prevent unauthorized access to identity properties.
IIQSAW-2640	[SECURITY]Upgraded Angular to version 1.7.9.
IIQSAW-2650	The plugin framework support for automatically running database scripts is limited to standard SQL statements. Database vendor specific commands will not work.
IIQSAW-2663	AccessRequestTypes containing a space that navigate to the Access Requests page will now render correctly.
IIQSAW-2671	TaskSchedule upgrader will upgrade the executor from id to name along with the existing upgrader logic to convert certificationDefinitionId from id to name.
IIQSR-175	Exceptions and errors no longer occur when opening the Scheduled Reports tab when the logged in user is an identity that is a member of more than 100 workgroups and scoping is enabled.

IIQSR-177	NativeChangeDetection information is no longer duplicated when multiple aggregations detect changes for the same identity and attribute.
IIQSR-178	All email templates now correctly support cc and bcc as template attributes.
IIQSR-179	Dialog windows for chained approval work items and other forms transition more fluidly.
IIQSR-180	Certifications that have self-managed managers are now correctly generated when creating global manager certifications.
IIQSR-187	When exporting a certification item, role application and role account names are now exported along with the rest of the data.
IIQSR-200	In the Correlation tab, under Edit Application, the **Edit** button is now disabled until the user selects a correlation configuration from the drop-down.
IIQSR-206	The content in the work Item details panel now appears on initial page load without requiring a refresh of the page.
IIQSR-211	Managing passwords for an identity is now possible without SQL parameter errors when using SQL Server and there are more than 2100 applications that support provisioning.
IIQSR-215	A warning has been added in the user interface when enabling file attachments that there is no file content validation or verification on attachments.
IIQSR-230	Links with null native identities no longer produce null pointer exceptions during aggregations when logging is turned on for rule: Rule-FrameWork-Correlation
IIQSR-231	Radio buttons on the Self Service Onboarding page will always have a default value rather than having no option selected.
IIQSR-234	The Workgroups editor now correctly displays the current page of members when one is added while viewing a page other than the first page.
IIQSR-236	The settings for **Leaver Options per Population** are no longer extended attributes and so will not appear on the Application definition pages.
IIQSR-244	Email notifications are now correctly sent for workitems detailing manual changes which are triggered from access requests on applications that do not automatically provision.
IIQSR-245	The workflow triggered from an Unlock Account when answering authentication questions now completes successfully, instead of an **Failed due to Invalid Request Type** or **Could not launch workflow** error.
IIQSR-248	Updated help text for Implicit Approval in Accelerator Pack global definitions to be clear about exceptions to the process to reduce confusion.
IIQSR-250	Attribute Synchronization is correctly launched when the identity has at least one account in the on-boarded application.
IIQSR-251	Some radio button options have been replaced with combo-boxes in the Self Service Onboarding form.
IIQSR-255	Notification emails for Lifecycle Events now correctly send emails to individuals when there is no group email and the notification setting is **Notify members only**.
IIQSR-259	Automatic approvals now work correctly when multiple approvers in LCM Provisioning approval scheme all automatically approve.
IIQSR-263	The Mover Lifecycle Event will now check if the Rehire, Joiner and Leaver Lifecycle Events are enabled before allowing them to supersede the Mover Lifecycle Event.

IIQSR-265	To improve the page's performance when loading on a system with many populations, IT Role Mining templates no longer pre-load all the population information in the system.
IIQSR-267	The Console About page now contains Accelerator Pack version information.
IIQSR-50	When the focus is on a postback field on a custom workflow form before clicking on the **Submit** button, two clicks are no longer required to submit the form.
IIQTC-53	Oracle DB users experiencing slow performance on the manage accounts screen should make the following changes to the UIConfig XML Object: **Note: retrieving the manager's displayName and ordering by displayName can affect performance** 1. Disable the initial rendering with this configuration: <entry key="disableInitialManageAccountsGridLoad" value="true"/> 2. Reduce the information displayed in the Cards by modifying the entry key "uiManageAccountsIdentityCard" elements.
IIQTC-169	On the IBM Tivoli Access Manager Application definition page, the help icons now display text, instead of nothing, while hovering.
IIQTC-171	When requesting access for an additional account, attributes with common values are not filtered out.
IIQTC-181	When there is a field in a form that has a pre-existing value that is not part of the allowed values, there will be a validation error when the form is submitted and the pre-existing value will remain, rather than allowing the pre-existing value to be submitted.
IIQTC-188	A Boolean checkbox in a custom form now supports the read-only setting.
IIQTC-189	Item and page counts for Task Results and Scheduled Tasks are now consistent with results displayed when performing a search or reset.
IIQTC-192	Reports are no longer duplicated across multiple pages in the worksheet view of My Reports.
IIQTC-195	Form refresh buttons can now be used to pass-in data for post-processing.
IIQTC-196	Filtered request items, are no longer improperly marked as failed.
IIQTC-198	Previously removed role assignments, will no longer affect display of required IT roles during access removal.
IIQTC-199	Application Integration Configurations, now persist maintenance window settings.
IIQTC-201	Group provisioning requests will correctly reflect status if the provision failed and is not being retried.
IIQTC-209	If a manager has a single subordinate, then that subordinate will be able to request access for themselves (instead of disallowing any request) using the LCM QuickLinks if the QuickLink allows for self service. In addition, a user without direct reports or subordinates should also be able to request access for themselves if the QuickLink allows for self service.
IIQTC-210	Application Dependency, no longer enforces dependency when deleting an Account.
IIQTC-216	The form text-area component shows the scrollbar in Microsoft Internet Explorer when the field is disabled, this change unifies the look and feel across Internet browsers.
IIQTC-217	Viewing a pre-existing workitem while interacting with a transient workflow no longer creates a NullPointerException.

IIQTC-218	Requests for scheduled attribute assignments with a sunrise date now provision as expected.
IIQTC-223	The Identity queries have been optimized to avoid using a low cardinality workgroup index.
IIQTC-236	During a Group Aggregation, the Account Group Description is correctly aggregated
IIQTC-241	The Audit Events actions Identity Added to Workgroup and Identity Removed from Workgroup now register the identity that made the change.
IIQTC-243	When using the Rule-Audit_Framework, the Scheduler can run Audit Rules without causing an error.
IIQTC-246	All birthright applications are now provisioned on rehire.
IIQTC-247	To improve some scoping queries, overlapping controlled scopes queries are optimized to only search against the relevant controlled scopes when and identity controls both a parent scope and one or more of its child scopes.
IIQTC-248	Certification beyond the Active Period, no longer display the **Undo Decision** and **Reassign** buttons.
IIQTC-250	The Advanced Analytics Identity search, is no longer limited to 100 elements.
IIQTC-259	Workitem filter **Owner** behavior, now searches based on exact word.
IIQTC-260	Approval Batch Requests, no longer fail.
IIQTC-264	Joiner Functionality, no longer requires the Native Identity in the Application Provisioning Policy.
IIQTC-267	In the Business Process Editor, modifying and previewing a form no longer results in an error when saving the workflow.
IIQTC-268	Expired work items will now auto-reject approvals.
IIQTC-269	Emails based on EmailTemplates with multiple recipients will be sent correctly rather than failing because of extra quotation characters.
IIQTC-271	SMTP servers that are slow to process requests will not hold up foreground task threads indefinitely. Instead, those threads will be sent into the Request Processor for retry.
IIQTC-275	Certifications that are configured to automatically close and are owned by workgroups are no longer blocked by an error when they are processed by the Perform Maintenance task.
IIQTC-278	Changes to the Accelerator Pack configuration no longer require a web container restart.
IIQTC-294	During an attribute sync with the Accelerator Pack, an identity can now contain multiple attributes with the same value and all accounts will receive an email during the sync.
IIQTC-297	Updated and moved the text in the onboarding forms from embedded xml to the `iiqCustom.properties` catalog, to improve clarity and readability and to allow for localization.
IIQTC-305	Audit Events of type Link Moved, now store Account Name and Native Identity in the correct fields.
IIQTC-313	SAML logins using a correlation rule that returns a link object will now successfully populate electronic signature forms with current user data.
IIQTC-315	With the Accelerator Pack installed, the Beta feature no long causes ApplicationExtended errors in the IdentityIQ console on startup.

IIQTC-317	The ColumnConfig for the Certification Detail View has been updated to reflect the Identity's DisplayName.
IIQTC-320	When processing Pending Requests, Task Results no longer throws a hibernate exception due to connection closed errors.
IIQTC-323	The reverse leaver workflow now continues to execute after a provisioning plan is executed.
IIQTC-328	Forgot password functionality configured with multiple pass-through applications now searches all configured applications for a valid user.
IIQTC-330	Email notifications in Accelerator Pack now expose the attributes of the accounts based on their priority. Whenever it applies, primary account attributes are exposed over privileged attributes but not the other way around.
IIQTC-331	A method in the NotificationRuleLibrary is no longer throwing null pointer exceptions when a Leaver process is triggered from a Termination.
IIQTC-337	When an identity's access is terminated using Terminate Identity Access all outstanding work items related to that identity are cancelled and removed from the system.
IIQTC-338	Exporting Advanced Analytic Searches, now export without intermittent errors.
IIQTC-339	Identity Creation from the Manage Identity page while using the default Create Identity LCM form now works correctly without error when **Run provisioning in the foreground** is disabled.
IIQTC-341	Role revocation or removal with overlapping entitlements, no longer results in multiple attribute requests for the same attribute.
IIQTC-346	Certification exclusion rules are now used when examining an identity that might become re-activated in the certification.
IIQTC-351	After an Upgrade, Certifications now display correctly when the Certification was created in the previous version and a Role contained with the Certification has been deleted prior to upgrade.
IIQTC-355	In Accelerator Pack, a request to clear an attribute value no longer results in an error.
IIQTC-359	Adding a new role without a name will no longer result in a NPE.
IIQTC-360	Bulk import of entitlement catalog no longer limits the imported file size to 1MB.