SailPoint IdentityIQ

Version 7.3

Release Notes

IdentityIQ Release Notes

These are the release notes for SailPoint IdentityIQ, version 7.3

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

This release note contains the following information:

IdentityIQ Feature Updates

IdentityIQ 7.3 provides new features and capabilities across the product, including Compliance Manager, Lifecycle Manager, the Governance Platform, and Connectivity. Key enhancements in the release include:

Process Resiliency

- Improvements in the following tasks: Aggregation, Certification Generation, and Identity Refresh
- Ability to specify a loss limit which enables administrators to start from the closest point of failure
- Ability to partition tasks and support restart with partitions for efficiency and reliability
- Support for resiliency under database failure
    - Ability to reanimate requests automatically or through the IdentityIQ console
    - Non partitioned tasks will be terminated immediately for efficiency

Environment Monitoring

- Single pane of glass for IGA administrators to get complete picture of IdentityIQ infrastructure as well as the connected ecosystem infrastructure
- Ability to monitor statistics on infrastructure:
    - CP
    - Memory
    - Latency to Database
    - Task Threads

  - Request Threads
  - Custom
- Ability to provide services on infrastructure:
  - Application heartbeat
  - Snapshot of statistics
  - Ability to configure the statistics and polling of statistics

Targeted Certification

- New certification type to enable a compliance officer to configure certification campaigns easily from the user interface
- Support for standard and extended attributes on identities, roles, entitlements and accounts to easily define the parameters of the certification campaign
- Ability to easily define a certification owner for identity types that do not have a manager, such as RPA/Bots
- Targeted certifications only support identity based certification or access reviews
- Pre-delegation rule within targeted certifications does not support reassignment
- Supports partitioning for better performance and scalability

Effective Separation of Duties Policy

- New policy type that enables you to define separation of duties (SoD) policy definitions on any access, direct or indirect
- All remediation actions on this policy will be handled through a work item requiring manual changes
- This policy definition will not be part of the preventative workflow as part of an access request, but will be included in a certification

Credential Cycling

- Enables administrators to leverage their privileged account management (PAM) applications' credential management capabilities in IdentityIQ
- Removes the need to manage privileged credentials in IdentityIQ and PAM applications
- Provides out of the box integration with CyberArk and BeyondTrust, as well as APIs to support other PAM solution integrations, to retrieve the privileged credentials from the PAM container for the accounts used to connect to target applications or systems. When in use, the credentials for those accounts no longer need to be entered and maintained in IdentityIQ.

User Experience Improvements

- New Approvals Page
  - The new approvals page shows all the approvals that are part of the access request flow
  - The responsive page shows all the approval work items, expanded, as well as the individual elements of that approval work item with the ability to bulk approve

  - The quicklink for this page is named Approve Access Requests and it is not enabled on the home page by default
- Work Item page
  - The work item page has been revamped to leverage the responsive user interface
  - Provides the ability to quickly view, search, and filter by the work items for efficiency
- Access Request improvements
  - The access request flow for self and others has been improved
  - The access request flow has clear numbering on the headers along with brief descriptions of what each step does, as well as a wizard like flow with a **Next** button to guide you through the steps
  - The access request page will now be shown blank by default with the **Search** and **Filter** buttons centered and more prominent, but you still have the option to view your entire catalog
  - The multiple user selection and de-selection has been improved as well. You can see the first 3-4 chosen identities. To see the complete list, click on any identity to open a popup that can be used to remove identities while still remaining in the current flow.
- Sign Off Improvements
  - Prompt for sign off feature has been re-introduced and is now enabled by default
  - Add an overlay that informs you if there are additional steps that need completion
  - Changes have been made to the My Access Review page. You will see a warning icon instead of 100% if there is work to be done

Governance of Robotic Process Automation (RPA)

- IdentityIQ is introducing a new standard attribute on the identity object. It is called Type and will support the following types of identities:
  - Employee
  - Contractor
  - Partner/External
  - RPA
  - Service Accounts
- RPA/Bot-type identity will also have two standard attributes provided by default
  - Administrator: An identity or workgroup that manages the bots
  - Software Version: To identify which version of the software the bot is running on
- The administrators of bots can do the following in IdentityIQ once the bots have been aggregated from an authoritative source:
  - Request access for bots
  - Certify access for bots using the new Targeted Certification
  - Manage the attributes of bots
  - Lifecycle changes on bots

Amazon Web Services (AWS) Governance Module

- Extend existing identity lifecycle and compliance management capabilities within IdentityIQ to mission-critical AWS IaaS environments
- Provides a central point of visibility, administration, and governance across the entire enterprise
- Enables policy discovery and access history across all organization accounts, provisioning AWS entities and objects, access review and certification, and federated access support
- Provides the ability to callout to AWS to retrieve the policy assigned to an identity cube and view the actual usage and content of the AWS policy.

SAP Governance Module

- Improves the user experience by introducing a new integrated visual interface for navigating and selecting SAP identities and roles as part of IdentityIQ's lifecycle management and compliance solution
- SAP data is presented in a familiar hierarchy format that closely resembles deployed system resources and organizational structures
- New filtering capabilities enable more efficient browsing and selection of SAP data so tasks can be performed faster. Improved granular support for separation of duty (SOD) violation policies provides flexibility for customers to craft more detailed identity governance policies that include SAP role details such as T-Codes and Authorization Objects

SharePoint Online Connector

The SharePoint Online Connector now supports managing multiple site collections in single application using REST APIs as Microsoft has announced deprecation of existing SOAP web services. The SharePoint Online Connector requires new application configuration details to connect to SharePoint Online using REST APIs. Ensure to update the required application configuration details of existing SharePoint applications after upgrading IdentityIQ to version 7.3.

Microsoft SQL Server Connector

The data model for the Microsoft SQL Server Connector has been enhanced. With this release, the Microsoft SQL Server Connector supports a new data representation: the Server Login will be the native identity on the account and the Database Logins, Database Roles, and Server Roles will be attributes on the account. Existing applications of type Microsoft SQL Server created before this update will continue to function with the previous data model and will need to be updated to take advantage of the new data model. The new model will be the supported path for this connector, while the previous data model will be supported for twelve months after the next major release of IdentityIQ. Please refer to the *SailPoint Direct Connectors Administration and Configuration Guide* for more detail.

The Microsoft SQL Connector now supports AlwaysOn feature for MSSQL high availability groups.

Active Directory Connector

The Active Directory Connector can now marginally enhance delta aggregation performance by adding a skipGetObjInMembershipDelta attribute in the application and setting it to true. This directs the connector not to perform an additional call to Active Directory to get complete object details for the objects for which changes are detected on memberships. The connector normally performs this additional get call in such scenarios to get more precise object counts that are displayed on the task result.

Open LDAP Connector

The Open LDAP Connector now supports provisioning entitlements with special characters in the Distinguished Name (DN).

To use this functionality, the following keys will need to be added to the application object:

```
<entry key="charsToEscapeInDN" value=",+\"<>;"/>
<entry key="charsToEscapeAtStartInDN" value="#"/>
<entry key="charsToEscapeAtEndInDN" value=" "/>
<entry key="charsToEscapeWhileProvisioning" value="/"/>
<entry key="convertHexToCharacter" value="true"/>
```

RACF Full Connector

Support for Connection attributes - With this feature, IdentityIQ has the ability to manage System Privileges (SPECIAL, OPERATIONS, AUDITOR and ROAUDIT) and Connection Privileges (SPECIAL, OPERATIONS and AUDITOR).

Configurations for Connection Privileges

1. The support for connection parameters can be enabled by performing the following:

1. Add the following attributes in the splConnectionAttributes section of the application debug page:
   `<entry key="CONNECTION_ATTRIBUTES" value="true"/>`

2. Apply the following PTF's on SailPoint Connector for RACF version 4.0.01:

   - FSD0083
   - FSD0084
   - FSD0085

Configuration for System privileges can be referred from *7.3 SailPoint Quick Reference Guide for Gateway Connectors*.

New Self Certification Reassignment Certification

A new Self Certification Reassignment certification has been implemented, with the owner of that certification being configurable both globally and at the certification group level. During certification generation as well as any certification refresh during its lifecycle, entities or items are moved to this certification if they otherwise would result in self-certification. Delegation work items are also forwarded to the same self certification reassignment owner if the delegation ownership would result in self certification, however the items and entities remain part of the original certification. Similarly, work items and certifications that are forwarded are reviewed prior to implementing the forward only when the option is enabled in Work Item settings. Otherwise, the forwarding will be allowed and the entities/items that are in violation will remain read-only until they are moved to the Self Certification Reassignment certification on next refresh. Self-certification by means of membership in a workgroup is prevented by making the affected items read-only, forcing another member of the workgroup to certify them.

New configuration options include the Self Certification Violation Owner (in the Compliance Manager and on the Advanced tab of the Certification Scheduler, only available for certification types involving identities); the addition of the ability to configure the Self Certification Allowed Level in the Certification Scheduler (again on the

Advanced tab), and the option to check for self certification on manual forwarding in the Work Item Rules section of IdentityIQ Settings.

These measures are also included in the new Targeted Certification scheduler.

Connectors and Integration Modules Enhancements

New Connectors

IdentityIQ 7.3 delivers new, out-of-the-box connectors for the following enterprise applications, which simplify connectivity of these systems.

Feature/Enhancement	Description	Benefits
New Connectors	Amazon Web Services (AWS) Connector	Amazon Web Services Governance Module manages the AWS Organizations entities such as Service Control Policies, Organization Units and AWS Accounts. It also manages the IAM (Identity Access Management) entities such as Users, Groups, Roles, Inline policies, Managed policies (AWS and Customer managed) under each AWS Account.
	SuccessFactors Connector	Manage Employee and Contingent workers from SuccessFactors Employee Central module using SOAP and REST APIs
	Okta Connector	SailPoint Okta Connector manages Users, Groups, Roles and Application using Rest API provided by Okta. Also enables single sign-on authentication across multiple applications and devices - even when they are behind firewalls or in the cloud.
	PeopleSoft Campus solution	PeopleSoft Direct Connector can now manage users and groups of PeopleSoft Campus Solution
	SAP S/4 HANA On Premise Module	SAP Direct Connector can now manage users and groups (R3) for S/4 HANA on premise module
	ServiceNow Service Catalog API Integration	SailPoint ServiceNow Service Catalog API Integration is an integration between ServiceNow and SailPoint IdentityIQ. This integration allows access request for roles using Service Catalog approach with ServiceNow user interface experience.

Active Directory

Connector	Features/Enhancements	Benefits
Active Directory	Supports strong authentication using SASL	Active Directory Connector now supports strong authentication between Active Directory and IdentityIQ using SASL framework, implemented with Kerberos.
	Support for managing Contact Objects	The Active Directory Connector now supports all the CRUD operations for contact including enabling\disabling exchange mail contact objects.
	Enhanced user interface to configure search scope and filters for contacts	Now you can define search scope for contacts object via UI.
	Supports less privileged Service Account to manage Skype for Business	Active Directory Connector now requires reduced permissions for managing the Skype for Business.
	Enhanced more efficient filters used to create partitions using auto-partitioning	Active Directory Connector is now enhanced to have more efficient filters used to create the partitions during auto-partitioning.

Azure Active Directory Connector

Connector	Features/Enhancements	Benefits
Azure Active Directory	Support Delta Aggregation for Accounts and Groups	Azure Active Directory Connector now supports delta aggregation feature which will bring delta changes related to accounts and groups.
	Support Partitioning in Delta Aggregation for Accounts	Added support for Partitioning in Delta Aggregation.

AIX Connector

Connector	Features/Enhancements	Benefits
AIX Connector	Support aggregation of last password change time	lastPasswordUpdated lets you know the details of when was the last password changed for a user.

Cerner Connector

Connector	Features/Enhancements	Benefits
Cerner Connector	Enhanced joiner process to support required attributes to create a Cerner account.	Added few more attributes to be updated while creating an account.
	Enhanced leaver process to support Disable Cerner account and set end date	Now connecter is supporting setup end date while terminating the user.
	Enhanced to use new SPML API for faster aggregation	Now using SPML APIs you can experience the faster aggregation.
	Support for aggregation and provision of personnelGroup attribute.	Added another attribute: personnelGroup.
	Added support for aggregation and provision of Credentials attribute.	Added another attribute: Credentials.

Connectivity Report

Connector	Features/Enhancements	Benefits
Connectivity Report	New report that collects application configurations and statistics	Connectivity Information Report - New report introduced that collects application configurations and statistics.

Duo Connector

Connector	Features/Enhancements	Benefits
Duo Connector	Support an optional attribute for assigning a phone to an account	Now you can attach Phone Type and Phone Platform while assigning Phone number to Account.
	Support User Alias	Added support for user Aliasing.

EPIC Connector

Connector	Features/Enhancements	Benefits
Epic Connector	Support Partitioning Aggregation for Accounts	For better performance and faster results, added support for Partitioned Aggregation for Accounts
	Enhanced User Interface for WS-Security configuration	Now you can configure WS security from user interface itself
	Support WS-Security core binding	EPIC Connector now also supports WS-Security for core binding WSDL.
	Supports StartDate/EndDate for Linked Templates	Added support for start date and end date for Linked Template.
	Supports aggregation and provisioning of additional attributes	Epic Connector now support aggregation and provisioning of additional attributes like EMP 20660 - Default Login Department EMP 20810 - Preferred Login Departments EMP 20820 - Login Department Filter List EMP 20830 - Login Department Filter Setting EMP 29080 - Report Authorized Service Areas EMP 29070 - Report Authorized Locations EMP 29060 - Report Authorized Departments EMP 29069 - Report Authorized Department Groups EMP 29075 - Report Authorized Providers EMP 29065 - Report Authorized User

GoogleApps Connector

Connector	Features/Enhancements	Benefits
GoogleApps/Gsuite Connector	Support transferring of associated data before deleting the account	Now you can retain the data of an employee when they leave the organization by transferring it to their managers account.
	Support for Delta Aggregation for Accounts and Groups	Now you can perform Delta Aggregation for Accounts and Groups objects
	Support for Role Assignments and Role Management	Now you can manage Roles using Google Apps Connector.
	Support aggregation and provisioning Custom Schema attributes	The Google Apps Connector now also supports provisioning of custom account schema attributes.

Multiple Application Builder

Connector	Features/Enhancements	Benefits
Multiple Application Builder	Connectivity enhanced to automate application creation to manage multiple hosts	This utility helps you create/update 100s of applications in minutes, saving time and manual efforts.

Microsoft SQL Server Connector (MSSQL)

Connector	Features/Enhancements	Benefits
Microsoft SQL Server Connector	Enhanced Data model	Data model of MSSQL Connector has been enhanced to support various aspects.
	Supports AlwaysOn feature for MSSQL high availability groups	Now also supports AlwaysOn feature for MSSQL high availability groups.

Mainframe Connectors

Connector	Features/Enhancements	Benefits
Mainframe Connectors	The RACF, ACF2 and Top-Secret Connectors support Password Phrase Interceptions	Password Phrase interceptions functionality helps to detect native changes and send it to IdentityIQ/IdentityNow for further synchronization
	The ACF2 Connector supports Automatic Group definition during Group Aggregation based on CA-ACF2 rules	It will assist to avoid manual work and automate group definition for aggregation
	The ACF2 Connector supports Rules/Groups Interception	It will assist to detect native changes of Rules/Groups happening on security system to be detected and sent to IdentityIQ/IdentityNow quickly. No need to run Account-Group aggregation for it.

Oracle E-Business Suite Connector

Connector	Features/Enhancements	Benefits
Oracle E-Business Suite Connector	Support for Future Hire	Added new aggregation filters like employees, contractors, employee and contractors and all users from FND_USER table in Oracle E-Business Suite to filter out data as per requirement.
	Support for aggregation filters for Employee, Contractors, Employee and Contractors, All EBS users	Added support for aggregation and provisioning of future dated employees and contractors.

Okta Connector

Connector	Features/Enhancements	Benefits
Okta Connector	Support for the filters in group aggregation	Now Okta Connector supports Group Aggregation Filter which helps to aggregate groups based on group filter.
	Adding support to uniquely identified request coming from IdentityIQ (SailPoint OKTA Connector)	Now onwards SailPoint REST requests to Okta will be identified uniquely using UserAgent as SAILOKTA/1.1 in the request header.

PeopleSoft Direct Connector

Connector	Features/Enhancements	Benefits
PeopleSoft Direct Connector	Supports PeopleSoft Route Controls	Now you can manage route controls too along with roles.

RACF Full Connector

Connector	Features/Enhancements	Benefits
RACF Full Connector	Support for managing group membership along with account properties	RACF-Full Connector now has ability to manage System Privileges (SPECIAL, OPERATIONS, AUDITOR and ROAUDIT) and Connection Privileges (SPECIAL, OPERATIONS and AUDITOR).
	Support for provisioning default group, account owner and connection owner	The RACF Full Connector now has the ability to set the owner and default group of a created or updated account.

RACF LDAP Connector

Connector	Features/Enhancements	Benefits
RACF LDAP Connector	Support for provisioning default group, account owner and connection owner	The RACF LDAP Connector now has the ability to set the owner and default group of a created or updated account.

SharePoint Server Connector

Connector	Features/Enhancements	Benefits
SharePoint Server Connector	Support filtering of site collections	SharePoint Server Connector now supports configuring application scope in terms of list of Site Collections that needs to be managed.

SharePoint Online Connector

Connector	Features/Enhancements	Benefits
SharePoint Online Connector	Rewritten using REST based API	Enhanced the connector with all new rest APIs
	Supports Azure Active Directory Groups	Now you can see Azure Active Directory group association.
	Multiple site collection in single application	The SharePoint Online Connector now supports managing multiple site collections in single application using REST APIs as Microsoft has announced deprecation of existing SOAP web services.

ServiceNow Connector

Connector	Features/Enhancements	Benefits
ServiceNow Connector	Supports Delta Aggregation for Accounts	Now you can perform Delta aggregation for accounts objects.

SAP HR/HCM Connector

Connector	Features/Enhancements	Benefits
SAP HR/HCM Connector	Supports Custom BAPI Invocation	Now you can invoke 2 custom BAPIs through this connector which can be used for filtering accounts and additional attributes.

Salesforce Connector

Connector	Features/Enhancements	Benefits
Salesforce Connector	Support for Freezing users	Salesforce Connector can now fetch the isFrozen state of a particulate salesforce account while doing account aggregation, the same can be updated via Identity IQ.
	Support Salesforce roles as group object	Now Roles are the new group object.
	Supports OAuth 2 Authentication	Now you can use OAuth2 mechanism for authentication.
	Supports permission set as group object	Salesforce Connector now supports permission set as group object.
	Support for filtering the frozen account	Now you can filter out frozen accounts during account aggregation.

System for Cross-Domain Identity Management Connector

Connector	Features/Enhancements	Benefits
System for Cross-Domain Identity Management Connector (SCIM)	Supports OAuth 2 authentication	Now you can use OAuth2 mechanism for building authentication
	Support for Complex Attributes	Added support for complex attributes which may have multiple values, like Phone, email, and so on.

System for Cross-Domain Identity Management 2.0 Connector

Connector	Features/Enhancements	Benefits
System for Cross-Domain Identity Management 2.0 Connector (SCIM)	Supports OAuth 2 Authentication with Refresh grant	SCIM 2.0 Connector now supports OAuth2 authentication mechanism using Refresh grant.
	Supports Filter for Account, Group, Role and Entitlements	Now you can add filters for Groups, Roles and Entitlements to manage only required data.
	Supports Client Credentials grant_type for authentication	SCIM 2.0 Connector now supports OAuth2 authentication mechanism using Client Credentials grant_type.

SuccessFactors Connector

Connector	Features/Enhancements	Benefits
SuccessFactors Connector	Introducing new configuration parameter odataEventOptionIdMap	Introducing new configuration parameter odataEventOptionIdMap which will decide the future hire to be aggregated based on the Picklist id event and the Identity status set as enabled or disabled based on the Picklistid employee-status.

Sybase Connector

Connector	Features/Enhancements	Benefits
Sybase Connector	Support for minimum permission for service account	Supports aggregation and provisioning by service account with minimum permissions.

UNIX Connectors

Connector	Features/Enhancements	Benefits
UNIX Connector	Supports aggregation of Sudoer commands for Accounts and Groups	Now Unix (Solaris, Linux, AIX) Connectors supports aggregation of sudoer commands for Account and Groups.
	Support for SSH key agreement scheme ECDH Curve25519 key exchange	Support for ECDH Curve25519 key exchange has been added and all the operations to be working fine.

WebEx Connector

Connector	Features/Enhancements	Benefits
WebEx Connector	Supports update of simple attributes	WebEx Connector now supports update of simple attributes.

Web Services Connector

Connector	Features/Enhancements	Benefits
Web Services Connector	Supports Pass Authorization for each end point	Web Services Connector will now use access token configured in the application as authorization header for each endpoint.
	Supports PATCH operations	Web Services Connector now supports PATCH operations.
	Supports OAuth 2 Authentication	Web Services Connector now supports OAuth2 authentication mechanism using Refresh grant.
	Support for Paging	Web Services Connector now supports generic paging for Account and Group Aggregations.
	Supports JWT Grant type for OAuth 2 Authentication	Now you can use JWT grant type for OAuth 2.0 authentication.
	Supports XML based request and response for Web Service API end points	Web Services Connector now supports XML-based request and response for web service API endpoints.
	Supports **Client Credentials** grant_type for authentication	Now you can use **Client Credentials** grant type for OAuth 2.0 authentication.
	Supports termination Provisioning, GetObject, Test Connection operation for before rule exception	WebSevices Connector now supports termination of Provisioning,GetObject and TestConnection operation for before rule exception.
	Supports terminating the aggregation based on user logic provided in Before/After rule	WebSevices Connector now supports termination of Provisioning,GetObject and TestConnection operation for before rule exception.

Workday Connector

Connector	Features/Enhancements	Benefits
Workday Connector	Support worker conversion cases independent of calculated field LATEST_WORKER_RECORD__c	Added handling for worker conversion cases independent of calculated field LATEST_WORKER_RECORD__c.

Connectivity Platform and Language Updates

Component	New Version
Connectivity	**ADAM Connector –** **-** ADAM Connector now supports Microsoft Windows Server 2016 **EPIC Connector –** - EPIC Connector now supports EPIC 2017 and EPIC 2018 **ITSM Connector –** - ITSM Connector now supports BMC Remedy IT Service Management version 18.05 **IQService –** **-** IQService now supports Microsoft .Net Framework version 4.7.x **JDBC Connector –** - JDBC Connector now supports Database deployed on AWS RDS **Linux Connector –** -Linux Connector now supports RHEL version 7.4 and 7.5 -Linux Connector now supports Ubuntu version 16.04 LTS **MSSQL Server Connector –** - MSSQL Server Connector now supports MSSQL Server 2017 - MSSQL Server Connector now supports MSSQL Database deployed on AWS RDS **Mainframe Connectors (RACF, ACF2 and Top-Secret) –** - The RACF, ACF2 and Top-Secret Connectors now support z/OS version 2.3 **Oracle Connector –** - The Oracle Connector now supports Oracle Database deployed on AWS RDS **Oracle Internet Directory Connector –** **-** Oracle Internet Directory Connector now supports Oracle Internet Directory version 12c **PeopleSoft Direct Connector –** **-** PeopleSoft Direct Connector now supports PeopleSoft Tools version 8.56 - PeopleSoft Direct Connector now supports PeopleSoft Campus Solution Module version 9.2 **Remedy Connector –** - Remedy Connector now supports BMC Remedy Action Request Sever version 18.05 **ServiceNow Connector –** - The ServiceNow Connector, ServiceNow SIM, and ServiceNow Launch in Context (LIC) solutions now support ServiceNow Kingston release **SAP Direct Connector –** - SAP Direct Connector now supports S4 HANA Module **SCIM 1.1 Connector –** - SCIM 1.1 Connector now supports Slack Server **Siebel Connector –** - Siebel Connector now support Siebel Server version 16.0 **SharePoint Server Connector –** -SharePoint Server Connector now supports Microsoft SharePoint Server version 2016

Connectivity Dropped Platform Support

Connector/Integration Module	Dropped Platforms
ServiceNow	The ServiceNow Connector, ServiceNow SIM, Helsinki, and ServiceNow Launch in Context (LIC) solutions no longer support the ServiceNow Geneva release
LNIX Connector	RHEL versions 6.6, 6.5, 6.3, 6.2, 6.1 and 6.0
Sybase Connector	The Sybase Connector no longer supports Sybase ASE versions 15.0 and 15.5.

Dropped Connector Support

The following connectors and connector components are no longer supported:

- AWS IAM Connector
- SharePoint Target Collector
- Lieberman Target Collector
- Microsoft Project Server

Important Upgrade Considerations

IdentityIQ 7.3 is a major release that contains numerous new features and capabilities across all areas of the product. A comprehensive plan should be created when upgrading that includes becoming familiar with the new features and changes, identifying use cases and how they are affected by the changes, creating a detailed strategy for migration of configuration and customizations, testing the upgrade process using data and system resources that are as close to the production environment as possible, and performing a complete deployment test cycle.

Object Model Upgrade

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

The changes include:

- Application

- For Google Apps applications, the encrypted attribute is changed to add clientSecret to the list of sensitive application attribute names.
- For SecurityIQ applications, values for the baseURL, alert.listEndpoint, alert.deltaListEndpoint, and alert.getEndpoint application attributes are moved to schema configuration attributes on the Alert schema.

Third Party Libraries

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

Cipher Mode for Encryption Changes

The cipher mode used for encryption of sensitive data was changed to CBC. This change is backward compatible with the exception of OAuth tokens referenced below and existing encrypted data using ECB cipher mode can still be decrypted. The Encrypted Data Synchronization task can be used to update all sensitive data to use the new cipher mode.

This change will invalidate all current OAuth tokens used for IdentityIQ API access. Any client using the SCIM API will need to be restarted or use client implementation specific mechanisms to request a new token after the IdentityIQ server has been started after the upgrade.

Deploying on Websphere Application Server, version 9

Additional steps are required during installation to achieve class loader isolation for IdentityIQ libraries when using WebSphere version 9. See the *SailPoint IdentityIQ Installation Guide* for additional information.

Continuous Certifications No Longer Supported

In IdentityIQ 7.3, the **Continuous** value in the Execution Frequency field of the Certification Scheduler is no longer supported. Previously defined continuous certifications will operate as usual. In a future release, certification campaigns defined with an execution frequency of continuous will not be supported.

Oracle EBS Connector

- When de-provisioning future entitlements, the Oracle E-Business Suite Connector now sets the end date of the assignment the same as the start date.
- During an aggregation or a provisioning operation through the Oracle EBS Connector, if the following error message is displayed:

  ORA-00942: table or view does not exist

  Provide additional permissions to the service account specified in the "Oracle E-Business Suite Integration Module" chapter in the *SailPoint Integration Guide*.
- The Oracle E-Business Suite Connector no longer aggregates indirect roles and responsibilities assigned to Oracle E-Business users during account aggregation by default.

Plugin Upgrades

Upgrading a plugin to the same version or a previous version is not supported. While developing a plugin, this behavior can be disabled for easier testing. To do so, include a `-dev` suffix on the version, for example, `2.0-dev`.

The version of a plugin can either be official or development.

Development versions end with the suffix `-dev`, for example, `2.0-dev`, and bypass most version checks so that the plugin can be recompiled, upgraded and tested easily.

Official versions drop the `-dev` suffix and can only be installed over a development version or an earlier official version. The minimum upgradeable version must also be valid.

Valid upgrade paths:

- 1.0 -> 2.0-dev
- 2.0-dev -> 2.0-dev
- 2.0-dev -> 2.0
- 1.0 -> 2.0

Invalid upgrade paths:

- 2.0 -> 2.0
- 2.0 -> 1.0

Password Reset and Account Unlock Messages

Several message keys are now available which can be optionally modified to give implementation specific error messages for certain password reset scenarios:

- `reset_err_user_not_found`: Message displayed when the user is not found
- `reset_err_no_sms_phone`: Message displayed when the SMS phone number is not set for the user or is in a bad format
- `auth_answers_not_configured`: Message displayed when authentication questions are not configured

A message key is now available which can be optionally modified to give an implementation specific error message during an unlock operation:

- `reset_err_user_not_found`: Message displayed when the user is not found

In order to see these messages in the UI, the user must have this SystemConfig setting: `<entry key="loginErrorStyle" value="detailed"/>`

Use of detailed login error messages must be weighed against internal security policies.

Supported Platforms

Operating Systems

Note: Linux Support: These 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) 7.3 and 7.4
- Oracle Linux (using RHE Kernal Mode) 7.3 and 7.4
- SUSE Linux 12.0 and 12.1
- Windows Server 2012 R2 and 2016
- Solaris 10 and 11

Application Servers

- Apache Tomcat 8.5 and 9.0
- Oracle WebLogic 12c Release 2 (12.2.1.x)
- IBM WebSphere 8.5.x and 9.0
- JBoss Enterprise Application Platform 7.0 and 7.1
- IBM WebSphere Liberty 18.0.0.1

Databases

- IBM Db2 10.5 and 11.1
- MySQL 5.6 and 5.7
- Microsoft SQL Server 2016 and 2017
- Oracle 12cR1 and 12cR2

Java Platform

- Java 1.8

Note: OpenJDK is not supported.

Browsers

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

- Google Chrome Latest Version
- Internet Explorer 11 and Edge
- Safari 11
- Firefox Latest Version

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

Mobile User Interface OS/Browser Support

- Android with Chrome 7 and 8
- iOS with Safari 11
- Windows with IE 10

Cloud Support

- AWS EC2
- AWS Aurora
- AWS RDS (MySQL, Microsoft SQL, Oracle)
- Azure

Languages

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

Resolved Issues

CONBOGIBEE-589	The RACF Connector now sets the requested group as the owner of the account entitlement.
CONBOGIBEE-633	Jive Connector now correctly provisions "Alternate Email" attribute if present in the schema and provisioning policy.
CONBOGIBEE-673	Jive Connector now correctly provisions "phoneNumbers" attribute if present in the schema and provisioning policy.
CONCHENAB-1908	Web Services Connector now support HTTP DELETE method with json payload.
CONCHENAB-1920	The OIM application now supports authentication for the IdentityIQ web application deployed on the WebLogic server.
CONCHENAB-1996	Salesforce Connector now supports case sensitive query filter with inner queries.

CONCHENAB-2050	The WebServices Connector now handles multiple aggregation requests triggered simultaneously.
CONCHENAB-2069	The Workday Connector now has a new flag 'Exclude Terminated Worker' to exclude the terminated workers from being aggregated.
CONCHENAB-2082	Workday Connector now handles multiple request / operations performed, using single Axis context.
CONCHENAB-2126	Webservices Connector now supports form-urlencoded request body.
CONCHENAB-2225	The AirWatch Connector now supports fetching records in chunks/pages.
CONCHENAB-2251	Salesforce provisioning now works for parallel requests.
CONCHENAB-2255	The Web Services Connector now supports complex JSON request payload containing placeholders.
CONCHENAB-2328	Workday Connector now will parse dates correctly even if time zone offset is after +5:30.
CONCHENAB-2350	Workday Connector now pulls the latest worker records for future hire even though if there are multiple records present for the same worker.
CONCHENAB-2355	Now Workday Connector takes care of empty attributes during aggregation.
CONCHENAB-2423	The Remedy Service Integration Module will now support special characters (&,<,>,",') in account and group attribute values.
CONCHENAB-2426	Web Services Connector now supports adding entitlements in create account operation.
CONCHENAB-2441	Webservices Connector now supports handling of String JSON Array.
CONCHENAB-2455	Now Workday Connector has provision to provide Effective date while updating contact details.
CONCHENAB-2457	LDAP SSL connection will now work even after performing test connection for Salesforce application.
CONCHENAB-2470	Workday Connector now populates the latest future records to the current status of worker during delta aggregation in case of the employee/ contractor conversion.
CONCHENAB-2559	The SCIM 2 Connector now request all resource types though resource types exceed more than 50.
CONCHENAB-2582	Remedy SIM now has configurable timeout per operation.
CONCHENAB-2585	RACF-Full Connector now supports operations through Cloud Gateway.
CONCHENAB-2594	Workday Connector now supports TLS 1.2 while connecting to the Workday system.
CONELLIS-1251	The AIX Connector now pulls in the last password reset details for an account.
CONELLIS-1513	**[SECURITY]** The Linux, Solaris and AIX Connectors now allow the disable.account application attribute value to use the usermod -s /bin/false command to truly disable users.
CONELLIS-1576	The Linux Connector no longer causes NumberFormatException when previewing and aggregating accounts.

CONELLIS-1688	Linux Connector has an option to not allow change password operation for disabled account.
CONELLIS-1837	Unix Connector now supports Sync Password for multiple account of identity.
CONELLIS-1900	AIX Connector no longer throws exception while changing password for root user.
CONELLIS-1922	The Siebel Connector now manages Siebel server connections more efficiently during account aggregation and no longer leaves stale connections.
CONELLIS-572	Now Unix Connector supports hmac-sha2-512 Cipher.
CONETN-136	The Open LDAP Connector now supports provisioning entitlements with special characters in the Distinguished Name (DN).
CONETN-1707	The Peoplesoft Connector no longer fails with Component Interface {CI_PERSONAL_DATA} error when jars are specified at multiple locations.
CONETN-1868	The SAP Connector now supports configuring load balancer properties from the UI.
CONETN-1891	SAP direct connector will now support provisioning of start and end date for role assignment when integrated with SAP GRC.
CONETN-1913	The Mainframe Connector no longer fails when aggregating and provisioning an account or group with '§' character in their names or attributes. The minimum version of Agent required for it to work flawlessly is Agent version 4.
CONETN-1955	The SAP HR Connector now aggregates Personal Number of a terminated employee during account aggregation.
CONETN-1971	The SAP GRC Integration now supports passing an additional parameter, simulationRiskOnly to the SAP GRC Proactive Risk Analysis Webservice.
CONETN-1987	The JDBC Connector no longer fails when merging columns using a driver that does not support scrollable result set.
CONETN-2014	The Delimited File Connector now successfully aggregates all accounts using SCP and a filename containing spaces.
CONETN-2021	The SAP HR Connector no longer fails with a NullPointerException when performing Delta aggregation.
CONETN-2044	The LDAP Connector now successfully provisions an account with a parenthesis in the Common Name (CN) within a Distinguished Name (DN).
CONETN-2050	The Oracle E-Business Suite Connector now updates the PASSWORD_DATE field of an account only during password reset request.
CONETN-2066	The Google Apps Connector now allows all special characters in a password while provisioning.
CONETN-2079	The Oracle E-Business Suite Connector now successfully aggregates accounts when using a service account other than APPS.
CONETN-2103	The Active Directory Connector now supports aggregating sIDHistory attribute and displays it in a readable string format.
CONETN-2116	The Active Directory Connector now updates msExchHideFromAddressLists attribute value in modify provisioning operation.

CONETN-2121	The Active Directory Connector now correctly saves in the application the state of the TLS communication option for a domain.
CONETN-2125	The LDAP Connector now saves delta aggregation key correctly after running full partitioned account aggregation.
CONETN-2129	The IBM Lotus Domino Connector no longer pulls in the account entitlements when the Groups attribute is removed from the account schema, thereby greatly improving the performance.
CONETN-2135	The JDBC Connector no longer causes Invalid column index error during Test Connection.
CONETN-2147	The Delimited File Connector no longer runs the post-iterate rule when previewing account or groups.
CONETN-2150	The Mainframe Connectors now correctly provision System Group attributes.
CONETN-2164	The PeopleSoft Connector no longer causes java.lang.NumberFormatException error for a change password operation.
CONETN-2167	SAP HANA Connector now supports dropping an account from the managed system for a delete provision request.
CONETN-2169	The Active Directory Connector now has a flag skipDeletedObjScopeCheckInDelta to configure whether or not the connector binds to deleted and recycled objects in Active Directory and processes them in IdentityIQ accordingly.
CONETN-2173	The Active Directory Connector no longer causes NoInitialContextException when aggregating accounts.
CONETN-2188	The Active Directory Connector now fetches group memberships according to the group membership filter string configured in application configuration for full account aggregation.
CONETN-2203	The Active Directory Connector now validates if Exchange Alias (mailNickname) is present in the provisioning plan before creating a mailbox for a user while performing an MS-Exchange modify provisioning operation.
CONETN-2205	The JDBC Connector no longer fails with "Unable to create iterator" exception during partitioned aggregation.
CONETN-2207	The IBM Lotus Domino Connector now correctly deprovisions when removing multiple groups in a role.
CONETN-2210	The Active Directory Connector now correctly provisions email and primary SMTP addresses for a MS-Exchange distribution group.
CONETN-2218	The Open LDAP Connector no longer fails when resetting password on Directory Server.
CONETN-2221	The agent-based connectors now retry every provisioning operation even
CONETN-2227	The Azure AD Connector now correctly removes the license pack if all the plans are removed from the pack, even if the user has multiple license packs assigned.
CONETN-2235	The Azure AD Connector now correctly aggregates different plans even if the plan ids are the same.

CONETN-2251	The Active Directory Connector now sets MS-Exchange attributes homeMDB and mailNickname as AD attributes if MS-Exchange is not enabled.
CONETN-2268	The Sybase Connector now also aggregates accounts from an offline database or a database created with for load option.
CONETN-2273	The mainframe connectors will now retry every account provisioning operation for all the retriable errors.
CONETN-2295	Microsoft SharePoint Server Connector no longer errors out in account aggregation even if there are only AD groups on the SharePoint server.
CONETN-2298	The Active Directory Connector no longer waits for user confirmation when updating one or more properties of a Skype account.
CONETN-2303	The mainframe connectors now also recognizes SKIP(1) as a success return code from the mainframe agent.
CONETN-2305	The Active Directory Connector no longer logs socket closed exception in SSL enabled pass-through authentication.
CONETN-2318	The Active Directory Connector now has improved logging in IQService while provisioning to MS-Exchange.
CONETN-2326	Sybase Direct Connector now supports aggregation by account with minimum permissions.
CONETN-2332	The Generic LDAP Connector no longer logs ObjectNotFoundException as an error in Pass through authentication.
CONETN-2359	The SAP Portal-User Management Web Service Integration Module now aggregates and correlates the correct account for every account provisioning request. 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 and correlation to work correctly.
CONETN-2365	The Active Directory Connector no longer fails with connection reset error in account aggregation.
CONETN-2367	The ServiceNow Connector no longer fails when updating email address of an account.
CONETN-2388	The Workday Connector will no longer log unwanted log traces as Error when performing aggregation of accounts.
CONHELIX-526	For the disable operation, the EPIC Connector will update the contact comment only once.
CONHELIX-671	The SCIM 1.1 Connector now supports pagination.
CONHELIX-743	The Okta Connector now supports a Group Aggregation Filter which helps to aggregate groups based on group filter.
CONHOWRAH-1148	The Active Directory Connector now binds to the correct secure port (636) during a retry when TLS is enabled and server less mode is configured.
CONHOWRAH-1270	The Active Directory Connector now has a flag aggregationMaxRetries for IQService to retry multiple times to get fastest DC in case of failures. Also, it has another flag skipBindUsingDNS to configure whether or not to fall back to binding using DNS in case binding using IQService to get fastest DC fails.

CONHOWRAH-1351	The Active Directory Connector can now marginally enhance delta aggregation performance by adding a skipGetObjInMembershipDelta attribute in the application and setting it to true.
CONHOWRAH-1352	While processing deleted objects during delta aggregation, the Active Directory Connector is now more resilient to bad data for isDeleted and isRecycled attributes.
CONHOWRAH-1354	The Active Directory Connector now has configurable attribute cacheSocketTimeoutMillis in application to specify socket timeout when caching is enabled.
CONNAMDANG-1030	When de-provisioning future entitlements, the Oracle E-Business Suite Connector now sets the end date of the assignment the same as the start date.
CONNAMDANG-1052	The Oracle E-Business Suite Connector now aggregates direct and indirect roles assigned to Oracle E-Business users during account aggregation.
CONNAMDANG-1055	The Oracle E-Business Integration Module no longer sets the Start Date of a user's entitlement to the current date when de-provisioning an E-business Role for the user.
CONNAMDANG-1062	The Oracle E-Business Suite Connector now uses future hire's start date
CONNAMDANG-1247	The Sybase Connector no longer supports Sybase ASE versions 15.0 and 15.5.
CONNAMDANG-1290	The Oracle EBS Connector now uses a combination of Responsibility_id and Application id to identify the responsibility group uniquely. Refer to the documentation on this connector if you have non-unique responsibility_ids in your Oracle EBS environment and want to use this feature for an existing application.
CONNAMDANG-990	The Oracle E-Business Suite Connector now has a new flag skipFutureAssignedGroups that influences how future-dated users are provisioned.
CONNAMDANG-993	Oracle E-Business Suite Connector now end-dates the user's entitlements when disabling a user.
CONNAMDANG-997	The Oracle E-Business Suite Connector no longer aggregates indirect roles and responsibilities assigned to Oracle E-Business users during account aggregation by default.
CONPAMBAN-1080	SharePoint Server Connector now supports configuring application scope in terms of list of Site Collections that needs to be managed
CONPAMBAN-460	The RSA Authentication Manager Connector now correctly populates the identitySource attribute details during the aggregation when present in the schema.
CONSEALINK-668	ServicNow Connector fails the provisioning of entitlement that does not exists on ServiceNow instance.
CONSEALINK-713	The ServiceNow Connector, ServiceNow SIM, and ServiceNow Launch in Context (LIC) solutions no longer support the ServiceNow Geneva release.
CONSEALINK-714	The ServiceNow Connector now builds the ServiceNow API URL without using double slashes.

CONSEALINK-724	The ServiceNow Service Integration Module is now following the proxy settings from the application server settings.
CONSEALINK-757	The ServiceNow Connector is now following the proxy settings from application server settings.
CONSEALINK-759	The ServiceNow Integration Module now has a configurable timeout for connector operations.
CONSEALINK-787	The ServiceNow Connector no longer support the ServiceNow Helsinki release.
CONSEALINK-788	The ServiceNow Service Integration Module no longer support the ServiceNow Helsinki release.
CONSEALINK-789	The ServiceNow Service Catalog Integration Module no longer support the ServiceNow Helsinki release.
CONUMSHIAN-1393	[SECURITY] API access via RESTful web services and the application command
CONUMSHIAN-1413	The SAP Integration Module no longer uses the application administrative credentials to validate login credentials during pass through authentication.
CONUMSHIAN-1753	New configuration parameter, odataEventOptionIdMap, to define if a future hire is aggregated based on the Picklist id event and the Identity status set as enabled or disabled based on the Picklistid employee-status. The odataEventOptionIdMap attribute has a default value set based on the values of Picklist id event and Picklistid employee-status, For more details Please refer to the "Additional configuration parameter" section in the "SailPoint SuccessFactors Connector" chapter of the *SailPoint Direct Connectors Administration and Configuration Guide*
CONUMSHIAN-992	The PeopleSoft Connector now supports aggregating User Profile attribute Route Control
IIQCB-1368	Added a details link to the component section of a work item which will allow for seeing more information about that work item.
IIQCB-1409	If the certifier is changed after a certification is scheduled, it will no longer default to the previous certifier.
IIQCB-1412	Added fix to not change delegated item status when making bulk decisions. The saved number will still reflect the total number of boxes checked, including delegated items in the list. No action will be taken, however.
IIQCB-1854	**[SECURITY]** Authentication to IdentityIQ web services will no longer accept encrypted passwords. All users must decrypt passwords prior to calling into these services. This will also apply to any use of Authenticator.authenticate(user, pass) made in beanShell.
IIQCB-1858	Updated the javadocs for sailpoint.object.identityrequestitem.
IIQCB-1896	Addressed cases where filtering for Manager on an identity certification would include non-managers.
IIQCB-1920	Double clicking **Login** no longer results in the login form getting reset and the login being abandoned.

IIQCB-1932	Saved searches from Advanced Analytics is now working more dependably by properly representing the searches and returning correct results.
IIQCB-1944	IdentityAttributeTarget type Rules input parameters have changed. An additional parameter link has been added to identify which link is being processed.
IIQCB-1945	The direct report widget now filters out inactive accounts.
IIQCB-1948	Updated translation based on feedback. Sign off button in German is now Rezertifizierung abschlieÃŸen instead of Abmeldeentscheidungen
IIQCB-1949	Updated some german translations based on feedback: MANAGE MY ACCESS (quick link and title): Zugriff > Zugang REVIEW AND SUBMIT (tab on manage my access page): Überprüfung > Überprüfen REMOVE ACCESS (tab on manage my access page): Zugriff entfernen > Zu entfernende Zugänge
IIQCB-1958	Some workflows were not properly handling password expiration. In particular, the Manage Passwords flow now respects the days until global preferences settings.
IIQCB-1969	Calling the sailpoint.tools.Util.otol() method with an empty object no longer throws a null pointer exception.
IIQCB-1972	Corrected an issue where 0/0 Completed Certifications displayed at 0% complete instead of 100% complete.
IIQCB-2020	Entering a backslash in fields of a provisioning form no longer causes an exception.
IIQCB-2021	Javadocs now includes information for sailpoint.api.passwordpolice.
IIQCB-2022	Improved error messages for electronic signature authorization to reference the invalid object type at the root of the error.
IIQETN-1581	The certification campaign wizard is now listing the certifications without duplicate entries.
IIQETN-2766	The Product Information section of the About page now shows information about any e-fixes installed.
IIQETN-3072	Saved searches from Advanced Analytics is now working more dependably by properly representing the searches and returning correct results.
IIQETN-4285	Native Change Detection no longer triggers for case insensitive applications when a modified attribute only differs in case.
IIQETN-4804	Role membership certifications will now be properly generated without errors when there are thousands of roles in the environment.
IIQETN-4849	The paging tool bar at the bottom of the grid will be reset to show the proper results when a new group of identities is displayed in the role mining population window.
IIQETN-4864	The Events tab of the identity view will correctly show a summary of single valued attributes that have been modified due to a native change.

IIQETN-4867	**[SECURITY]** Certification tags are now filtered of malicious content to prevent a possible XSS vulnerability.
IIQETN-4891	A role configured to provision both a capability and entitlements now correctly generates a provisioning plan with the entitlements in it, rather than only provisioning the capability.
IIQETN-4960	The displayed completion percentage for a certification group is now consistently calculated.
IIQETN-5085	The Policy Violation Review is now always displayed when requesting access even when there are previously existing violations.
IIQETN-5086	The Perform Maintenance task is now more aware of expired Work Items that were previously locked.
IIQETN-5135	The creation of task results with the same name across multiple threads is now less likely to result in exceptions associated with name collisions.
IIQETN-5161	Background provisioning on a workflow with approvalSplitPoint enabled that is run with multiple Perform Maintenance threads no longer duplicates provisioning.
IIQETN-5243	Comments on role requests that generate manual work items will be displayed on the approval and now the manual workitems too.
IIQETN-5408	In the Lifecycle Manager settings, the **Manage Account** option now has the desired impact when there are mixed combinations of enabled and disabled options.
IIQETN-5445	Additional account link data can now be displayed in both the Manage Accounts and Manage Passwords pages.
IIQETN-5481	The My Reports tab on the Reports page now uses pagination to better accommodate a large number of reports.
IIQETN-5485	Account selection rules are now run when assigned roles are modified and changes propagated.
IIQETN-5529	User-based searches when requesting access should be faster in most cases. Setting the option lcmMaxRolesFromUserSearch to an integer in the system configuration can further limit the number of roles fetched.
IIQETN-5543	The Account Group Members Report now correctly handles result sets that are greater than the reportingResultRowThreshold setting in SystemConfiguration.
IIQETN-5544	The lastRefresh date is now normalized for all accounts during partitioned aggregation to avoid time synchronization issues.
IIQETN-5554	The display name is now added to the managed attribute when an entitlement is promoted to a managed attribute in the Missing Managed Entitlement Scan.
IIQETN-5561	The paging control on the role configuration page now shows the correct number of pages when switching between the definition of different roles.
IIQETN-5563	Accounts are now correctly optimized during aggregations of Google Apps applications.
IIQETN-5579	Canceling a certification should not result in a full table scan for IdentityEntitlements associated with the certification.

IIQETN-5580	The audit logging format for errors logged from a running service is now more consistent for all types of audit events.
IIQETN-5668	Restrict recursion when tracing code that may have self-referential values.
IIQETN-5681	When an account attribute is changed both in the native application and in the user interface, the precedence of those changes is now correctly determined.
IIQETN-5699	In the Entitlement Catalog, sorting now works in the Members tab for managed attributes.
IIQETN-5740	Pass-thru authentication now works when more than one application account has the same native identity, even when they are on different applications.
IIQETN-5744	Oracle full table scans are now prevented on the Manage Work Items page.
IIQETN-5747	The Role Details Report no longer displays duplicate entries when filtering on applications.
IIQETN-5797	In Manage User Access, permitted roles now show for inherited roles in the list of requestables.
IIQETN-5854	When access is requested, a forwarding operation record will be logged on the workitem history when a default forwarding user has been specified for the identity owning the access.
IIQETN-5872	When editing or adding an entitlement in the entitlement catalog and **Refresh On Change** is enabled, the description on the group no longer loses its content.
IIQETN-5883	When viewing an access review using a link from another access review, the built-in **Back** button now returns the user to the original access review.
IIQETN-5899	The certification delegation email template now includes a parameter to make reference to the work item.
IIQETN-5923	**[SECURITY]** The extended attribute fields in the role editor are now filtered to prevent an XSS vulnerability.
IIQETN-5933	Role provisioning forms are now only displayed once when approvals are disabled and approvalSplitPoint is set to a non-null value.
IIQETN-5937	When viewing roles with the tree view disabled, the grid is now displayed correctly after a role is deleted, and no longer causes a hang in the user interface.
IIQETN-5943	Certification work items that are over a day past their expiration now expire properly.
IIQETN-5959	**[SECURITY]** The configuration page for assignment rules on the role editor now prevents content that can exploit an XSS vulnerability.
IIQETN-5960	**[SECURITY]** The advanced view for attribute rules and permissions in the role editor will now prevent content that can exploit an XSS vulnerability.
IIQETN-5961	Identity entitlements are now correctly displayed when the identity name contains special characters, such as a plus sign.
IIQETN-5973	Role population stats can now be disabled during user-based access request searches by setting the new system configuration variable lcmDisableRolePopulationStats to true.
IIQETN-5977	When no data is returned in a search in Advanced Analytics, the generated PDF/CSV report now contains header information.

IIQETN-5982	Propagating a role name change no longer results in the user losing an assignment.
IIQETN-5983	Unnecessary updates to Bundle objects are no longer performed during a call to the Provisioner compile method which can happen during a provision or an Identity Refresh task.
IIQETN-6001	Role change approval work items now correctly contain a link to the Role Editor page for non-role managers.
IIQETN-6002	Account attributes that reference groups are once again properly displayed and will allow a click to show more details where enabled.
IIQETN-6013	**[SECURITY]** Hidden password fields now have autocomplete disabled.
IIQETN-6052	The Perform Maintenance task configured with the **Automatically close certifications** option now correctly processes delegated items.
IIQETN-6054	Waiting work items are no longer duplicated for split provisioned requests that are waiting for an integration to complete.
IIQETN-6062	Role Membership Certifications include membership information for each targeted account within a single Identity.
IIQETN-6076	System Maintenance task results now provide warnings when workflow threads time out. The results now contain the number of workflows processed as well as the number of timed out workflows.
IIQETN-6088	The Debug -> Connections page will now show the thread id, name, and created date of connections and the Perform Maintenance task now contains more debug statements with the thread id and name.
IIQETN-6098	A sunrise/sunset that has been edited on other approvals now is reflected in each work item that shares the same approval item.
IIQETN-6100	A role assignment that has been included in the identity risk score is now properly removed from the score when de-assigned.
IIQETN-6101	The Role Archive Report now shows accurate values for the Enabled field when it is run only for disabled roles.
IIQETN-6105	**[SECURITY]** Nested HTML tags are now filtered of malicious content to prevent a possible XSS vulnerability.
IIQETN-6119	When editing a role and using the Advanced view in Entitlements, changing the entitlement profile description will be correctly persisted after saving.
IIQETN-6122	Detectable roles that are required by roles that are also required by other roles are now properly annotated with their corresponding role assignment.
IIQETN-6139	An approval for an access request associated with an inactive role owner is now properly forwarded to the manager of the role owner.
IIQETN-6140	An extraneous submission of a WorkItem completion no longer leads to duplicated processing of that WorkItem.
IIQETN-6141	Validation errors added to an approval now display on the approval page.
IIQETN-6151	An Identity Refresh task with **Maintain Identity Histories** selected no longer incorrectly updates identities with sunrise roles to show the role to be currently assigned.

IIQETN-6154	Authentication answers are now trimmed of any surrounding whitespace characters.
IIQETN-6159	The session timeout now correctly performs a ping to the web server without using authorizations. This can also prevent a warning after acknowledging a session expiration message.
IIQETN-6165	The Action Status column on the Manage Accounts screen now shows the correct provisioning status, when the provisioning operation is different from the current status of the account in the Status column.
IIQETN-6169	The LCM Provisioning workflow variable workItemComments now correctly adds only one comment instead of duplicate comments.
IIQETN-6171	The Business Process Editor now correctly displays buttons when creating a form and the browser language is configured as non-English.
IIQETN-6187	Both the display value and the actual value of an entitlement will be shown in the approval for either a remove request or an add request.
IIQETN-6198	The identity search fields and suggest drop-downs now correctly return results when searching for identities that include a backslash in their first name, last name or display name.
IIQETN-6209	Aggregation of applications with multiple group schemas no longer leaves connections open.
IIQETN-6220	Exporting to CSV the content of an Advanced Certification based on Population no longer results in an error.
IIQETN-6231	An application defined with the NO_AGGREGATION feature string now displays in the list of applications on the Application Definition page.
IIQETN-6240	**[SECURITY]** When editing an access review, the certification group id is now encoded to prevent an XSS vulnerability if the user visited a compromised URL and returned to the access review.
IIQETN-6250	Assignments associated with multiple roles are now properly removed.
IIQETN-6252	Ampersands are no longer escaped multiple times when importing XML.
IIQETN-6254	Under Setup -> Tasks, the Scheduled Task tab now correctly displays all pages.
IIQETN-6256	Identity history is now correctly displayed when the identity name contains special characters, such as a plus sign.
IIQETN-6257	A role name containing an apostrophe character now displays correctly.
IIQETN-6260	Role descriptions are now maintained if the role name is changed.
IIQETN-6275	Certification items for deleted entitlements now display correctly and no longer prevent the loading of the remaining items.
IIQETN-6276	Waiting work items are no longer duplicated for split provisioned requests when items are approved and an expired work item exists for the request.
IIQETN-6279	When assigning a role with a provisioning form that references a deleted application, a warning message is now logged instead of a NullPointerException.
IIQETN-6286	When configuring access request search criteria in Advanced Analytics, the Request Type now shows the list of possible LCM request types.

IIQETN-6317	Under Advanced Search of the Certifications page, the Tag drop-down list now shows all entered tag values.
IIQETN-6336	The Identity Refresh workflow now contains a step to save changes to an identity to avoid the creation of duplicate work items.
IIQETN-6344	Multiple work items that are simultaneously processed for the same access request no longer cause database deadlocks.
IIQETN-6345	Database deadlocks no longer occur when work items from a request are purged at the same time other work items from the same request are being processed.
IIQETN-6363	Content displayed in a workflow form column will now wrap so the adjacent column information is not overwritten.
IIQETN-6367	Two options on an Approval step in a workflow have been provided so that end users will not see ObjectAlreadyLocked exceptions if the workitem is locked when completing an approval workitem.
IIQETN-6371	Setting the arguments foregroundProvisioning and doRefresh to true in the Compile Project step of the Identity Update workflow no longer causes a ClassCastException when editing an Identity.
IIQETN-6382	Role change events are no longer deleted if a problem occurs when attempting to propagate the changes described in the event.
IIQETN-6383	Viewing an item in the Manage Access page for an Account Disable operation now displays the correct Action Status.
IIQETN-6385	Identity requests with multiple policy violations will not revert changes upon submission with violation.
IIQETN-6398	In SAML SSO enabled environments, a misconfiguration no longer leads to an infinite loop on `setTimeZone.jsf`. This looping would occur if the URL entered into the browser does not match the URL entered in the SAML metadata on the SSO identity provider, which is typically caused by not consistently using fully qualified domain names. Under these circumstances the user will now be redirected to the login page and an appropriate warning message logged.
IIQETN-6414	The display name field is now shown in the approval item summary of changes for a role change only if it has actually changed.
IIQETN-6418	Removing required roles in the Role Editor no longer results in an error.
IIQETN-6419	Provisioning forms will not provision entitlements from an existing account on the same identity when submitting to a new, secondary account when the native identity is calculated.
IIQETN-6427	**[SECURITY]** The Identity Risk Scores page now prevents a cross-site scripting attack through modification of a request.
IIQETN-6428	Within the Risk Scoring Configuration page, the Composite Scoring -> Certification Age screen, the values for the certification offset and the certification range are now required fields, preventing a system exception when later revisiting the page.
IIQETN-6429	Completed Access Reviews for non-administrator users no longer appear in the open access reviews list.
IIQETN-6432	When making an account-only request, ensure only applications supporting account-only are displayed.

IIQETN-6441	Viewing a role composition certification no longer results in an error after comments are added to other certifications.
IIQETN-6451	Updated Turkish translations based on customer feedback.
IIQETN-6458	Viewing a role composition certification no longer provokes an identity history table scan and a possible page timeout.
IIQETN-6460	Entitlement Analysis results created with an OR filter are now correctly exported to CSV when the results contain an account with a null display name.
IIQETN-6481	When the system configuration option disableInitialAccessRequestGridLoad is configured to disable the initial Access Request page load, it no longer restricts an identity search performed using only the filters.
IIQETN-6487	In a multithreaded scenario where one thread has modified the scorecard or entitlement group of an Identity while another thread is attempting to lock the same identity, appropriate steps will be taken to allow the second thread to lock the identity and proceed without errors.
IIQETN-6497	An IntegrationConfig without a created date is now loaded and cached properly.
IIQETN-6519	When viewing an Identity, roles configured to not be detected will not show as such when required by an assigned role.
IIQETN-6623	Fixed issue which prevented some Chinese, Japanese and Turkish localized messages from displaying.
IIQETN-6629	In the Advanced Certification screen, removing populations from the certification schedule no longer obscures the view of other currently assigned populations.
IIQETN-6634	Encrypted passwords are no longer accepted for any method of authentication.
IIQETN-6641	The Role Editor now preserves Identity names which contain consecutive white space characters.
IIQETN-6662	The loading spinner and session timeout dialog now correctly localize to the current language without requiring the browser cache to be cleared.
IIQETN-6760	Overlapping requests to remove the same entitlement does not result in the entitlement remaining on the Identity with the Missing status.
IIQMAG-1270	The tooltip for Policy Violation Owner in the Rule Editor has been revised to accurately reflect the supported return values, which are String - identity name; Identity - identity object.
IIQMAG-1294	The error message presented when a password change fails, has been improved for clarity.
IIQMAG-1308	**[SECURITY]** Cipher mode for encryption was changed to CBC.
IIQMAG-1309	An enhancement has been added to filter the list of identities and entities in an access review through the panel on the left side of the screen, accessible by clicking the people icon at the top left of the access review.
IIQMAG-1316	To eliminate ambiguity in the list view of certification items, in addition to display name, email address is now provided.
IIQMAG-1320	The SCIM2 Connector no longer presents an Unsupported Media Type error when the connection to an OIM system is tested.

IIQMAG-1321	Adding or deleting identities in a Workgroup is now an audit event and appears in the audit log.
IIQMAG-1337	The Identity Object Service RESTful call to return a list of identity suggestions no longer fails with a 413: Request Entity Too Large error.
IIQMAG-1339	The form field now supports a POST method. We added a POST method for the `rest/suggest/object/{class}` endpoint. The GET endpoint was left in place; however, if the query parameters would make the URL too large, POST can be used as an alternative.
IIQMAG-1422	Certification items are no longer duplicated across multiple pages in the worksheet view of a certification.
IIQMAG-1491	It is now possible to search identities based on Assigned Role in the Lifecycle Manager.
IIQMAG-1685	The Work Items page now preserves sort and filtering choices. If the list of work items is sorted or filtered (or both), and the user navigates to the individual work items from the list, when they return to the list, the filters and sort order are retained. Navigating away from Work Items to another part of the IdentityIQ user interface will have the effect of clearing the sort and filter settings.
IIQMAG-1774	Performance of the My Access Request page has been improved due to database query optimization.
IIQMAG-1783	The **Enable password auto-generation when requesting for others** option in Lifecycle Manager configuration now disables the **Generate** button in Manage Passwords when changing the password for an identity.
IIQMAG-1789	The count now accurately reflects the number of accounts changed in cases where new passwords are generated for all accounts in a change password provisioning policy for an application.
IIQMAG-1902	Type is now translated in the Type column of Entitlements Catalog, the Type filter drop-down when advanced searching the Entitlement Catalog, in the page title when creating a new entitlement, and in the Type drop-down when creating a new entitlement.
IIQMAG-1903	Forms using a dynamic radio button now properly display both the radio button and the field value.
IIQMAG-1905	When Group By is enabled, bulk decisioning of a large group of certification items now properly applies the decision to all items in the group, even when the items in the group span multiple pages.
IIQPB-431	Having populations with no members will no longer cause failures during Identity Refresh.
IIQPB-433	Removed the `javax.xml.namespace.QName.class` files from the `jaxrpc.jar` and `xpp3.jar` files shipped with IdentityIQ to prevent class loading conflicts during rule execution.
IIQPB-438	Changes to logging in `log4j.properties` will now take effect without server restart or manually clearing the cache. The logging config change will take effect within X seconds, where X is the period of the Cache Service defined in the Configuration object under the key cachedObjectDuration.

IIQPB-440	When viewing Roles, the Top Down and Bottom Up trees will also show roles which are not in your scope. However, the roles which are out of scope are read only.
IIQPB-441	Fixes have been made to improve querying the audit table when it has a large number of records. Column indexes are automatically detected and queries are optimized appropriately.
IIQPB-442	Addressed issues where multiple, duplicate manual provisioning work items are created for the same user during subsequent Identity Refresh tasks. The system now tracks workflows for each user to prevent these. It is possible to revert to the old behavior by adding the following option to your Identity Refresh task: <entry key="noCheckPendingWorkflow" value="true"/>
IIQPB-443	Changes have been made to reduce instances of secret attributes being displayed when using trace level logging.
IIQPB-446	Improvements were made to database indexing to improve the load time for the list of identities on Identity Warehouse page.
IIQPB-455	All workflow variables priority are now renamed to workItemPriority. We previously would set workItemPriority for every sub-case to the parent's value. You can now override this in the step args.
IIQPB-463	Specifying multiple approvers in a Lifecycle Manager workflow should no longer result in an object not found error. The product was not properly handling CSV inputs for this field.
IIQPB-467	Entitlements will now show as Granted by Role when the role granting the entitlement is part of a hierarchy.
IIQPB-492	An application of type SecurityIQ now allows textboxes in the user interface to set the username and password in the Alert Configuration.
IIQPB-554	**[SECURITY]** API access via RESTful web services and the application command line console is now protected by correct authorization and authentication.
IIQPB-556	Corrected issue which caused deadlocks during split provisioning workflows.
IIQPB-563	Encrypted passwords will no longer be stored in Provisioning Transaction objects.
IIQPB-564	Properly assign trackingIDs to items requested to prevent duplicate assignment during split provisioning workflows.
IIQPB-565	Deleting a Certification from the console is now more efficiently using available computing resources.
IIQPB-568	RoleMetaData objects will no longer be resolved by name during refresh. This prevents errors from being logged that were not indicative of actual issues during the process.
IIQPB-617	A new capability has been added to the product called ViewAdminConsole. This allows a user to see the Hosts, Tasks, and Provisioning Transactions pages of the Administration Console.
IIQPB-649	CSRF validation is now correctly provided for web service endpoints related to Work Item assignment.
IIQPB-655	Changes have been made to prevent passwords from appearing in trace level logging.

IIQPB-659	The version of Apache Commons FileUpload used by IdentityIQ has been updated from 1.3.2 to 1.3.3.
IIQPB-671	Approval Mode (serial or parallel) is now honored during Lifecycle Manager workflows for all Approval Schemes.
IIQPB-672	The version of the Spring Framework used by IdentityIQ has been updated from 4.3.5 to 4.3.16.
IIQPB-681	Support for lock names has been removed to avoid confusion between identifiers.
IIQPB-684	The link which was previously located under Gear -> Global Settings -> Host Configuration as been replaced by Gear -> Administrator Console -> Environment Monitoring.
IIQPB-718	Targeted certifications do not support pre-reassignment rules. Instead, you should use the new owner rule. This, other delegation related settings, and access-review specific settings (**Approve Options**, **Revoke Options**, **Allow Options**) can be found under the Additional Settings tab, Advanced Options panel.
IIQPB-719	Corrected a situation where usernames and encrypted passwords were displayed in trace logs.
IIQSAW-1237	Date field normalization has changed. All date selections will now be set to midnight based on the logged in user's timezone. Daylight Savings Time will be correctly applied for historical dates. Previous normalization logic has been removed. Browser timezone detection logic has changed to use new Intl.DateTimeFormat interface through moment-timezone library.
IIQSAW-1238	**[SECURITY]** The web service that provides content for identity suggest components now supports whitelists for objects and columns. If any custom code used the REST endpoint at `/ui/rest/suggest`, it will need updated system configuration values for suggestColumnWhitelist and suggestObjectWhitelist to list the object and columns that will be allowed to be queried.
IIQSAW-1239	Error messages in Advanced Analytics can now be localized.
IIQSAW-1240	The contents of the Manual Changes Requested page in the Lifecycle Manager and the value of the Activity Monitoring flag in the Identity Warehouse can now be localized.
IIQSAW-1243	To support localization of the values in the Action drop-down of Advanced Analytics Audit search, both the action name and display text is now shown in the drop-down.
IIQSAW-1245	Role Assignment and detection information is now stored in the certification item attributes map at time of generation and used in the certification item table and details dialog for role items. This means that if assignment information changes during the certification lifecycle the information in the certification will remain a point in time. Any certification created pre-7.3 will not have this information present and will show current assignment information in all cases.

IIQSAW-1249	If you have an embedded form in a Workflow/Business process and you use Auto Layout to layout the steps, the contents of the embedded form are now preserved.
IIQSAW-1252	When an access request results in manual provisioning for an application that is enabled for Native Change Detection, a native change event is no longer generated the next time aggregation and refresh tasks run.
IIQSAW-1255	It is now possible export Tag objects on their own or as part of CertificationDefinition. When importing CertificationDefinition with tags into 7.3, new tag objects are created (if they do not already exist).
IIQSAW-1281	Upgrading a plugin to the same version or a previous version is no longer supported. While developing a plugin, this behavior can be disabled for easier testing. To do so, include a `-dev` suffix on the version, for example `2.0-dev`.
IIQSAW-1285	When the Remediation attribute of an application is set to **Select**, the display value of the attribute is displayed instead of the value.
IIQSAW-1290	Reports with titles containing umlauts can now be successfully attached to emails.
IIQSAW-1337	Roles containing the ampersand character (&) are now rendered correctly in the user interface.
IIQSAW-1373	The Continuous value in the Execution Frequency field of the Certification Scheduler is no longer supported. Previously defined continuous certifications will operate as usual. In a future release, certification campaigns defined with an execution frequency of continuous will not be supported.
IIQSAW-1384	Date labels in the Certification scheduler are now localized.
IIQSAW-1661	Additional measures have been introduced to eliminate self-certification.
IIQSAW-1856	**[SECURITY]** RichFaces resources are now filtered to address a vulnerability. Custom code using RichFace components may be affected, especially if any custom page uses mediaOutput component.
IIQSR-12	Processes that generate BOM files now reliably function consistently when generating a custom WAR file.
IIQSR-14	In the Manage Access request screens, the details window for roles now has a new tab called Allowed Roles, which displays required and permitted roles for the selected role and roles from which it inherits.
IIQSR-15	Role mining results that contain an "&" character in entitlements no longer cause exceptions.
IIQSR-16	Permitted roles may now be associated with more than one already assigned business roles that permit them.
IIQSR-18	When all roles that reference an entitlement are revoked from an identity in an access review, the entitlement is now removed from the identity.
IIQSR-19	Form fields with special characters in their names now render combo boxes correctly
IIQSR-25	Full Text searches can now use a configurable analyzer that allows administrators to specify their own delimiters, allowing indexed documents to be tokenized at custom word boundaries.

IIQSR-26	Several message keys are now available which can be optionally modified to give implementation specific error messages for certain password reset scenarios.
IIQSR-27	A message key is now available which can be optionally modified to give an implementation specific error message during an unlock operation.
IIQSR-28	In Advanced Analytics the boolean operator for multiple advanced identity search filters is preserved after making changes to
IIQSR-29	In Advanced Analytics, selected Entitlement extended attributes are now included in exports to CSV and PDF.
IIQSR-3	Start Date and End Date now correctly show on the Provisioning Engine section of an access request detail screen, rather than being blank.
IIQSR-30	The Detailed Provisioning Transaction Object Report now runs successfully when there are no ProvisioningTransaction objects saved.
IIQSR-32	The Mobile Violation Reviews Quicklink is now only available in new instances if LCM is enabled.
IIQSR-33	Certification forwarding rules once again no longer execute for certifications containing items for members of the certifying workgroup.
IIQSR-4	Deleting a workgroup in the user interface is now prevented when the workgroup is set as the Identity value for the Policy Violation Owner of any SOD Policy Rule.
IIQSR-5	The Application editor no longer intermittently changes schema attribute types when navigating quickly between Application configurations that might differ.
IIQSR-7	The Application editor no longer intermittently changes schema attribute types when navigating quickly between Application
IIQSR-8	Workflow and Request Theads in the process of sending e-mails now time out gracefully if there are environmental network or server problems.
IIQTC-16	The Subtitle field of the Forms Sections now supports localization.
IIQTC-19	Launching a transient workflow through a QuickLink no longer generates an exception.
IIQTC-20	A SAML Correlation rule can now return a Link as an alternative to an Identity.
IIQTC-21	The Hibernate session is checked to see if it is closed before attempting to close it, preventing unwanted error messages.
IIQTC-22	A link that happens to be added because of refreshing an identity as a side effect of the Perform Identity Request Maintenance task will not cause a failure due to a ConcurrentModificationException.
IIQTC-23	A policy violation resulting from an access request now properly displays conflicting roles for Violation Summary in the Violation Details tab.
IIQTC-30	Access Request Id is now shown in the Work Item Details tab in PAM Approvals.
IIQTC-31	Negative role assignments are no longer restored during role change propagation.
IIQTC-4	When extending the Active period of a certification, the remediation WorkItem notification configurations are properly recalculated.
IIQTC-42	Under Setup -> Tasks, the Scheduled Task tab now correctly displays all pages.

IIQTC-8	The Detailed Provisioning Transaction Object Report now correctly displays errors generated during provisioning.
IIQTC-9	A sunrise/sunset date that has been edited on other approvals is now reflected in each new workitem.