SailPoint IdentityIQ

Version 8.0

Release Notes

IdentityIQ Release Notes

These are the release notes for SailPoint IdentityIQ, Version 8.0

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 8.0 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 8.0 introduces the following new features or enhancements. For a more detailed description of the changes, see

Feature/Enhancement	Description
Integration with IdentityAI for Decision Recommendations	IdentityAI is SailPoint's SaaS identity analytics solution. Using artificial intelligence and machine learning, IdentityAI gives you deeper visibility into managing risks associated with user access. IdentityIQ version 8.0 provides the first out-of-the-box integration with IdentityAI, enabling you to use IdentityAI's insights for guidance in access reviews and access request approvals
Automatic Deprovisioning of Expired Roles and Entitlements, with Notifications	Improved functionality and consistency in how IdentityIQ handles expired roles and entitlements, including optional email notification of impending sunsetting/deprovisioning of roles and entitlements, and the option to add sunset dates with automatic deprovisioning when exceptions are present during certification access reviews.
File Attachments in Access Requests	Access requests can now include file attachments, on an optional or a required basis. For example, you could attach training certificates or a notarized document of authorization.

Feature/Enhancement	Description
Responsive Approvals - User Interface Enhancements	An expanded default view for Approvals provides full information for all approval items, making it easier for approvers to review and process access requests from a single page, without having to click through to items individually in order to see details and take action.
Plugin Improvements	Enhancements to plugins include the ability to leverage classes contained in plugins from any area or feature of IdentityIQ from which BeanShell can be used. For example, rules, workflow steps, and scriptlets. This version also adds support for the use of forms in plugins, which gives you new ways to present complex or dynamic options in the plugin's configuration.
New Context-Sensitive Help	New context-sensitive help has been added to the product for Targeted Certifications, Access Reviews, and Access Requests.
Changes to Logging	Version 8.0 of IdentityIQ uses version 2 of Log4j, which adds new logging capabilities (specifically, change listening), and changes the logging configuration file name and logging syntax.
Support for Piped Commands in the IdentityIQ Console	IdentityIQ 8.0 adds support for piping to `iiq console` commands, providing useful ways to filter or redirect output.
Application Builder	Supports creation or update of applications based on provided schema and provisioning policies in the input **.csv** file. This enhancement supports bulk schema changes for different applications.

Connectors and Integration Modules Enhancements

New Connectors

IdentityIQ version 8.0 delivers new, out-of-the-box connectors for the following enterprise applications, which simplify connectivity of these systems.

New Connectors	Description
Workday Accounts	SailPoint IdentityIQ Workday Accounts Connector aggregates Workday Accounts records from Workday and enable/disable the Workday Account.
Oracle Fusion HCM	SailPoint IdentityIQ Oracle Fusion HCM Connector aggregates the employee and contingent worker records from Oracle Fusion HCM cloud service.

Amazon Web Services

Connector	Description	Benefit
Amazon Web Services	Aggregates **Password Last Used** date and **Access Key Last Used** details for every IAM User	Enhanced to bring additional attributes which are required to be kept for usage

Box

Connector	Description	Benefit
Box	Supports delta aggregation for Accounts and Groups	Enhanced to handle change set in delta aggregation, no need to rely upon full aggregation every-time

Cerner

Connector	Description	Benefit
Cerner	Support for Phone and Address attributes	Additional attributes added to display phone and address associated with an personnel
	(Dormant Account support) Supports the functionality of removing an username or disassociating an account	Enhanced to handle dormant accounts for better identity governance

Connector Gateway

Connector	Description	Benefit
Connector Gateway	Enhanced and optimized TLS communication between IdentityIQ and Connector Gateway	Enhanced and optimized TLS communication between IdentityIQ and Connector Gateway

Duo

Connector	Description	Benefit
Duo	Support pagination parameters as per Duo guidelines	Enhanced to handle pagination in API calls which is recently introduced by Duo
	Supports aggregation and provisioning of Duo administrator users	Enhanced to manage administrator users along with regular users
	Supports minimum permission for Test Connection operation	Connector can now be configured using fine grained permission with respect to associated transaction in which customer is interested

Epic Healthcare

Connector	Description	Benefit
Epic Healthcare	Supports configurable **UserID** type for Web Services administration	Enhanced to support configurable parameters to handle different level of mapping

G Suite (Google Apps)

Connector	Description	Benefit
G Suite	G Suite is the new name for the connector type formerly called Google Apps.	Connector type Google Apps is now renamed as G Suite
	Supports fetching assigned roles to user during account delta aggregation	G Suite Connector will now bring roles related changes in delta aggregation, now there is no need to depend upon full aggregation for these changes

IBM Security Identity Manager

Connector	Description	Benefit
IBM Security Identity Manager	Supports provisioning of (IBM Security Identity Manager) ISIM roles	Enhanced to manage full role provisioning and de-provisioning operations

IQService

Connector	Description	Benefit
IQService	IQService now offers enhanced security of the communication channel between IdentityIQ and IQService using TLS and client authentication. Using this mechanism now all transactions are well authenticated and encrypted. Applications of all connectors that uses IQService now have **IQService User** and **IQService Password** fields which are mandatory for IQService configured to communicate over TLS. For enhanced security, this release of IQService now requires Client Authentication to be configured to process any request that it receives on TLS port.	IQService is offering OOTB enhanced security as per industry standard. Using this mechanism now all transactions are well authenticated and encrypted

Microsoft SharePoint Server

Connector	Description	Benefit
Microsoft SharePoint Server	Supports **Exclude Site Collections** filter to define application scope	Customers now can define scope for sites which they do not want to manage in Microsoft SharePoint Server connector using **Exclude Site Collections**

Oracle

Connector	Description	Benefit
Oracle	Supports network encryption and data integrity features for the Oracle Database	Enhanced to handle Standard Security recommended by Oracle
	Supports secure connection for Oracle Database	Enhanced to support OOTB security with SSL, no other customization is required
	Manages users and groups of Oracle 12c and 12cR2 for container database (CDB) at current container level. There is no change in support of Pluggable database (PDB) for Oracle 12c and 12cR2	Enhanced the connector to manage users and groups on container level

Oracle ERP – Oracle E-Business Suite

Connector	Description	Benefit
Oracle ERP – Oracle E-Business Suite	Supports network encryption and data integrity features for the Oracle Database	Enhanced to handle Standard Security recommended by Oracle

Okta

Connector	Description	Benefit
Okta	Supports log API instead of Event API for delta aggregation	Enhanced with correct level of APIs to handle the deprication of older APIs
	Improved aggregation performance	Enhanced with better performance for especially aggregation related transactions.

PeopleSoft HCM Database

Connector	Description	Benefit
PeopleSoft HCM Database	Supports DB2 as backend database	Enhanced to support PeopleSoft with DB2 as database

SAP HR/HCM

Connector	Description	Benefit
SAP HR/HCM	Improved aggregation performance for multiple **Action Type** configured	Enhanced the connector with optimized call to handle multiple action type. Reduced 70% of calls and connector is now aggregating data 70% faster

SAP ERP - SAP Governance Module

Connector	Description	Benefit
SAP ERP - SAP Governance Module	Enhanced to support SAP Business Warehouse Module	Enhanced to support different SAP Modules
	Enhanced to support SAP Customer Relationship Management (CRM) Module	
	Enhanced to support SAP Process Integration (PI) Module	
	Enhanced to support SAP GRC Module	
	Enhanced to support SAP FIORI	
	Supports Aggregation of **Authorization Objects** associated with the roles	Aggregates another granular level of permissions called as **Authorization Objects** associated with roles

Salesforce

Connector	Description	Benefit
Salesforce	Supports public group as a group object. This enables aggregation of all the public groups, irrespective of, if they are not attached to any account.	Enhanced to support the aggregation of Public Group as a separate group object. Which enables wider governance on Public groups not even associated with users.

System for Cross-Domain Identity Management 2.0

Connector	Description	Benefit
System for Cross-Domain Identity Management 2.0	Supports delta aggregation for accounts, groups, roles, entitlements	Enhanced to support delta aggregation, users can now detect change set from delta aggregation only

SuccessFactors

Connector	Description	Benefit
SuccessFactors	Supports aggregation of termination date	Enhanced to bring **Termination Date** as separate schema attribute. No more customization is required to handle back dated entries

Sybase

Connector	Description	Benefit
Sybase	Supports aggregating **password_expiration_interval**, **password_expired**, and **expire_login** attributes	Enhanced to handle additional attributes OOTB, which will enable users to configure password Intervals

SAP HANA

Connector	Description	Benefit
SAP HANA	SAP HANA Connector now has the ability to fetch the terminated accounts	Enhanced to handle terminated accounts and customer can choose from which date they want to aggregate terminated accounts

SAP ERP - SAP Portal - User Management Web Service

Connector	Description	Benefit
SAP ERP – SAP Portal - User Management Web Service	SAP Portal is now enhanced with more secure integration library	Enhanced with more secure integration library. To leverage this functionality Customer must redeploy the `sailpont_ume.sda` file

Web Services

Connector	Description	Benefit
Web Services	Support for Pass Through Authentication	Enhanced for Pass Through Authentication
	Support for multiple group objects	Enhanced to handle multiple groups objects which enables better control over applications with complex data models
	Supports client certificate authentication	Enhanced to support another level of authentication supported by several managed system
	Supports saving of updated refresh token received from target system in the application	Updated refresh token received from managed system can be saved for easier connection configuration

Workday

Connector	Description	Benefit
Workday	Support for Parallel Aggregation	Enhanced to handle multiple threads to improve the overall performance of connector
	Supports all the filters supported by version 30.1 of the Workday API. The filters must be added to the response group filter in the upgraded application	Enhanced to support additional filters
	Support for Organizational level filters	Enhanced to support advance filtering, now customer can choose the data set with filters in which the customer is interested
	Support for minimum permission in Workday version 31.0	Connector now offers granular level permissions to operate with Workday version 31.0
	Supports option to set 'auto complete' as true while updating contact information	Enhanced to handle **auto complete** operation while doing provisioning operations. No separate customization is required

Connectivity Platform and Language Updates

Connector/Component	New Platform Version
Solaris	Solaris Connector now supports Solaris version 11.4 SPARC x86
Linux	Linux Connector now supports Red Hat Enterprise Linux version 7.6
RACF LDAP	RACF LDAP Mainframe now supports IBM Tivoli Directory Server for z/OS 2.3 with SDBM LDAP back end
MicroFocus Service Manager Service Desk	MicroFocus Service Manager Service Desk now supports Micro Focus Service Manager 9.6
ServiceNow	The ServiceNow Connector, ServiceNow Service Desk, ServiceNow Catalog and ServiceNow Catalog API IT Service Management Infrastructure Modules support the ServiceNow Madrid and London release
DB2	DB2 Connector now supports DB2 database installed on Linux
SAP HANA	SAP HANA Connector now supports SAP HANA 2.0 SPS3
BMC Remedy Service Desk	BMC Remedy Service Desk IT Service Management Infrastructure Module now supports BMC Remedy AR System Server version 18.05

Connector/Component	New Platform Version
LDAP	• LDAP Connector now supports Novell e Directory (NetIQ) version 9.1 • LDAP Connector now supports Microsoft ADAM version 2019
Workday	Workday Connector now supports workday API version 30.1
AirWatch	AirWatch Enterprise Mobility Management now supports version 9.5.0.16
Epic	Epic Healthcare now supports EPIC version 2019
Active Directory	• Active Directory Connector now supports Microsoft Windows Server 2019 • Active Directory Connector now supports Microsoft Exchange Server 2019
Sybase	Sybase Connector now supports HADR (High Availability Disaster Recovery) SAP ASE 16.0 SP03
RSA Authentication Manager	RSA Authentication Manager Connector now supports RSA Authentication version 8.1 SP1 and onwards
Microsoft SharePoint Server	Microsoft SharePoint Server Connector now supports Microsoft SharePoint Server version 2019
PeopleSoft HCM Database	PeopleSoft HCM Database Connector now supports DB2 as backend database
SAP GRC	SAP GRC Application Module now supports SAP GRC Access Control version 12.0
SAP ERP - SAP Governance Module	SAP ERP - SAP Governance Module is now certified with SAP S4/HANA on premise version 1809
IQService	IQService now supports Microsoft Windows Server 2019

Connectivity Dropped Platform Support

Connector/Integration Module	Dropped Platforms
ServiceNow	The ServiceNow Connector, ServiceNow Service Desk and ServiceNow Catalog IT Service Management Infrastructure Modules no longer supports the ServiceNow Istanbul release
	The ServiceNow Connector, ServiceNow Service Desk and ServiceNow Catalog IT Service Management Infrastructure Modules no longer supports the ServiceNow Jakarta release
ArcSight IT Security	The ArcSight IT Security Information And Event Management Infrastructure Module no longer supports the HP ArcSight Enterprise Security Manager version 6.8
Microsoft SQL Server	The Microsoft SQL Server Connector no longer supports the Microsoft SQL Server versions 2014 and 2012

Dropped/Deprecated Connector Support

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

- CyberArk Connector
- Novell Identity Manager Provisioning Integration Module
- Microsoft Project Server
- Sun Identity Manager Provisioning Integration Module
- Lieberman Integration Module
- BMC Remedy Service Request Management Adapter Service Catalog Integration Module

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

- Jive Connector
- SharePoint Unstructured Target Collector for Active Directory
- Microsoft Forefront Identity Manager

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

Important Upgrade Considerations

IdentityIQ Version 8.0 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:

- **Certification Column Upgrader**: This changes the Access Review user interface to use targetDisplayName from the certification entity for the Identity display name instead of doing a join to the Identity table every time.
- **Continuous Certification Upgrader**: Continuous certifications are no longer supported. This upgrader transitions any existing continuous certifications into periodic certifications. Items are set to the active period and appropriate phase transitions are set up based on the settings of the continuous certification definition.
- **Dashboard Upgrader**: The IdentityIQ dashboards, My Dashboard, Compliance Dashboard, and the Lifecycle Manager, are no longer supported. This upgrader removes SPrights and dashboard content as well as other things related to these dashboards.
- **Plugin Upgrader**: Changes were made to expand functionality of the Plugin Framework. This upgrader sets the relaxPluginExportDeclarationEnforcement key to `true` in System Configuration to allow previously installed plugins implementing custom Task, Service, or Policy executors to function as before. See “Plugin Upgrades” on page 14.
- **Quicklink Upgrader**: This upgrader removes the Access Request Approvals quick link introduced in 7.3. All approval types are now implemented in the new style and the Approvals quick link will now take you to the updated page. See “Approval Consolidation” on page 16
- **Request Notification Needed Upgrader**: This upgrader sets the notificationNeeded flag on existing requests with a nextLaunch attribute.
- **UI Work Item List Card Upgrader**: This upgrader updates the UIConfig columns for the Work Item list card. Previously some fields on this page were hardcoded and could not be configured by changing UIConfig.

IQService

For enhanced security, this release of IQService now requires Client Authentication to be configured to process any request that it receives on TLS port.

Applications of all Connectors that uses IQService now have **IQService User** and **IQService Password** fields. These fields are mandatory for IQService configured to communicate over TLS.

SAP ERP - SAP Governance Module and SAP HR/HCM

With this release of IdentityIQ 8.0, Test Connection might fail with an error even when all the required libraries are there in the required (WEB-INF\lib) path for the IdentityIQ host. To resolve this issue, follow the steps mentioned in ‘Troubleshooting’ section of the following:

- SAP ERP - SAP Governance Module in *SailPoint Integration Guide*
- SAP HR/HCM in *SailPoint Direct Connectors Administration and Configuration Guide*

IBM JDK 1.8

With this release of IdentityIQ 8.0, **Test** connection might fail for connectors which are connecting to target systems that are configured over TLS 1.2, for example, Okta, SucessFactors, Oracle Fusion HCM, and SalesForce with IBM jdk 1.8.

To resolve this issue, set the value of system property `com.ibm.jsse2.overrideDefaultTLS` to `true` in java.

Web Services Applications

IdentityIQ 8.0 supports the Client Certificate Authentication feature. For existing Web Services applications to use the Client Certificate Authentication feature, add the following attributes to the csv value of the encrypted attribute in the application:

```
clientCertificate
clientKeySpec
```

Connector Classloader

IdentityIQ 8.0 supports separate classloader for Connectors. Custom Connectors can use it to avoid the impact of IdentityIQ third-party library change/upgrade.

After upgrading IdentityIQ, Custom Connectors and Customization Rules can be impacted if connectors are initiated directly without using Connector Factory.

For example, `connector = ConnectorFactory.getConnector(application, null);`

SQL Server Snapshot Isolation Enabled by Default

In IdentityIQ 8.0, snapshot isolation in SQL Server is enabled by default in the database upgrade scripts to matches the database creation scripts. The enabled settings are:

- `ALLOW_SNAPSHOT_ISOLATION`
- `READ_COMMITTED_SNAPSHOT`

This facilitates locking without excessive blocking. As a result of this change, you can expect an increase in the use of the SQL Server `tempdb` resource.

UIConfig File Property Reference Changes

In IdentityIQ 8.0, property references to Identity.displayName in the following `UIConfig` file entries are replaced with parent.targetDisplayName.

- "uiCertificationItemWorksheetColumns"
- "uiTargetedCertificationItemWorksheetColumns"
- "uiCertificationItemReturnedItemsColumns"
- "uiTargetedCertificationItemReturnedItemsColumns"
- "uiCertificationItemPolicyViolationsColumns"

The CertificationColumnUpgrader is part of the changes to address deleted identities in the certification user interface. The goal of the upgrader is to replace references to Identity.displayName in the certification item columns to parent.targetDisplayName, so the value is included even if the identity is deleted.

JSONDeserializerFactory class Deprecation

The change to improve the security in JSON deserialization has introduced a stricter and more accurate parsing syntax for JSON data. Any custom code or integration that generates JSON outside of IdentityIQ might need to be updated.

In IdentityIQ 8.0, the JSONDeserializerFactory class has been deprecated. The deserialize and deserializeList methods remain, but only pass through to the JsonHelper.

The FlexJSON JSONDeserializer class has also been deprecated. Any custom code or rules should be updated to eliminate any use of the FlexJSON JSONDeserializer class or the JSONDeserializerFactory class, and instead use the JsonHelper class. All JSON inputs must be properly formed with keys and string values surrounded by either single or double quotes.

Expired Password Reset Configuration

In IdentityIQ 8.0, the **Requiring Current Password** option for the Expired Password Reset process can be configured on the Passwords tab of Configure IdentityIQ Settings page. This setting defaults to not required during an upgrade from a previous version of IdentityIQ, but defaults to required for new In IdentityIQ 8.0 installations.

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.

This release contains a large number of upgraded third-party libraries. Some changes in these libraries contain API changes that are not backward compatible. If custom code or rules use these libraries directly, the use might need to be updated. Indirect use through the published SailPoint API is not be impacted.

Plugin Upgrades

Note: For complete information on working with plugins, refer to the SailPoint IdentityIQ *Administration Guide*.

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

Plugin Version Requirements

Note: The single exception to these changes are version numbers with -dev appended to the end. This suffix causes version number validation to be bypassed. Attempted plugin upgrades to versions that do not support this pattern may fail depending on how the version number is interpreted.

To provide better support for upgrading plugins, we have set new requirements for plugin version number formats. Plugin version numbers must be numeric, contain no alphabetic or other characters, and separate the elements of the version number with decimal points. Within each segment of the version number, the values between the decimal points, the values are cast as integers, and leading zeroes are trimmed.

For example:

- `04` and `00004` are both interpreted as `4`
- A segment containing any non-numeric values is interpreted as `0`
- `1.004.alpha` is parsed as `1.4.0`
- `2.3.4a` will be parsed as `2.3.0`

To change the version of a plugin, you must change the contents of the `manifest.xml` file, which is contained within plugin's ZIP file. Within the `manifest.xml` file, the version is an attribute of the `<Plugin>` element in the XML.

For example:

```
<Plugin … name="MyPlugin" …  version="1.3" >
```

The steps to change the plugin version are:

1. Unzip the `.zip` file into an empty directory
2. Edit the extracted `manifest.xml` file
3. Change the value of the version attribute. For example, change from 1.3 to 1.4
4. Save the change to the `manifest.xml` file
5. Compress all of the files, recursively, in the directory, including the modified `manifest.xml`, into a `.zip` file

The `.zip` file you created can now be installed into IdentityIQ.

Explicit Class Declaration in Plugins

Note: During upgrade to 8.0, the Relax strict declaration enforcement option is set to true if there are any existing plugins.

In IdentityIQ 8.0, plugin classes that are used for TaskExecutor, ServiceExecutor, and PolicyExecutor must be declared in the plugin manifest as explicitly available for the TaskExecutor, ServiceExecutor, and PolicyExecutor. At run-time, instantiation of the classes validates that they were declared properly.

To allow existing plugins to work as they did in previous releases, select the **Relax strict declaration enforcement** option on the Global Settings->IdentityIQ Configuration -> Miscellaneous tab under the gear icon.

If this option is not selected, the loading of classes from plugins for TaskExecutor, ServiceExecutor, and PolicyExecutor is only be permitted if the `manifest.xml` for the plugin explicitly declares those classes to be exported.

Prohibit Scripts From Access Plugin Loaded Classes

IdentityIQ 8.0 provides a way (on a running system) to prevent all scripts from being able to call out to classes loaded from plugins.

To prevent all scripts from accessing classes loaded from all plugins, select the **Prohibit scripts from accessing plugin-loaded classes** option on the Global Settings -> IdentityIQ Settings -> Miscellaneous tab.

IdentityIQ Dashboards No Longer Supported

In IdentityIQ 8.0, all IdentityIQ dashboard components have been removed. This includes My Dashboard, Compliance Dashboard, and the Lifecycle Manager Dashboard.

New Version of log4j

IdentityIQ has updated to a newer version of log4j. All previously configured logging or other customizations related to `log4j.properties` must be manually moved to `log4j2.properties`. The syntax has also changed.

https://community.sailpoint.com/docs/DOC-13381

Approval Consolidation

In IdentityIQ 8.0, all approval workitems are handled in the same way, from the same page. Access requests are no longer handled separately.

If you have a custom quicklink named approvals, it will be overwritten during an upgrade. You should always give custom quicklinks unique names when they are created.

Credential Cycling (or AIM) Integration for CyberArk

In IdentityIQ 8.0, the credential cycling (or AIM) integration for CyberArk uses methods that use HASH as the authentication mechanism to ensure that they are passed securely. This requires that you run a CyberArk utility to generate the hash.

Richfaces are Replaced with Primefaces

In IdentityIQ 8.0, Richfaces was replaced with Primefaces. Any custom pages that relied on a4j components will need to be updated to instead use an appropriate Primefaces or JSF component.

Changes to the MySQL Create Script

In IdentityIQ 8.0, the syntax for the create user statements in the MySQL database script `create_identityiq_tables-8.0.mysql` has changed.

If you use a tool that changes the `create_identityiq_tables-8.0.mysql` script (to use a different MySQL username, password, or database name), you must update that tool to use the new syntax.

Approval Work Item Changes

In IdentityIQ 8.0, the following changes were made to approval work items:

- Any work item of type ViolationReview, Form, or Approval will be rendered by the newer AngularJS rendering engine.
- Any work item of type Approval or Form will affect the notification count in the upper right portion of IdentityIQ.
- Any custom approval step in a workflow must set the forceClassicApprovalUI argument to true if the custom form used in the approval has dependencies on ExtJS and/or the original custom form renderer released in version 6.x

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) 7.5 and 7.6
- Oracle Linux (using RHE Kernel Mode) 7.5 and 7.4
- SUSE Linux 12.1 and 12.2
- Windows Server 2016 and 2019
- Solaris 10 and 11
- CentOS 7.5 and 7.6

Application Servers

- Apache Tomcat 9.0 and 8.5
- Oracle WebLogic 12.2.1.x
- IBM WebSphere 9.0
- Jboss Enterprise EAP 7.2
- IBM WebSphere Liberty 18.0.0.4

Databases

- IBM DB2 10.5 and 11.1
- MySQL 5.7 and 8.0
- MS SQL Server 2016 and 2017
- Oracle 18c, 12cR2
- 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 8 and 9 with Chrome
- iOS 12 with Safari

Cloud Support

- AWS EC2
- AWS Aurora
- AWS RDS
- Azure VM
- Azure Azure SQL

Languages

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

- Traditional Chinese
- Turkish

Resolved Issues

CONBOGIBEE-859	The Jive Connector now correctly aggregates all accounts from native Jive system.
CONCHENAB-2681	The Workday Connector now aggregates only one record for a worker with multiple records.
CONCHENAB-2706	The Cloud Gateway now successfully connects to Active Directory forest.
CONCHENAB-2771	The Workday Connector now generates a new token after it is expired when updating custom attributes.
CONCHENAB-2849	The Workday Connector now no longer causes NullPointerException for an exception with an empty message.
CONCHENAB-2850	The Dropbox Connector now supports transferring files of a terminated dropbox account to the target dropbox account.
CONCHENAB-2853	The System for Cross-Domain Identity Management 2.0 (SCIM 2.0)Connector now correctly parses Latin characters.
CONCHENAB-2859	The Workday Connector now uses Workday Server time instead of system time to avoid failures which were due to time mismatch when running delta aggregation.
CONCHENAB-2875	The Workday Connector now no longer removes the termination date for an account when aggregating it on the day of the termination.
CONCHENAB-2880	The Okta Connector now no longer fails for delta aggregation when aggregating an empty attribute value from native Okta system.
CONCHENAB-2893	The SCIM 2.0 Connector now supports meta attribute while creating an account.
CONCHENAB-2903	The SCIM 2.0 Connector now supports meta attribute on the ServiceProviderConfig endpoint.
CONCHENAB-2909	The System for Cross-Domain Identity Management (SCIM) Connector now supports connecting to HTTP proxy server.
CONCHENAB-2915	The SCIM 2.0 Connector now does not discard java.lang.NullPointerException if SCIMObject schema attribute is null.
CONCHENAB-2922	The SCIM Connector now supports Identity Correlation for primary attributes.
CONCHENAB-2926	While running delta aggregation, Workday Connector now picks up correct worker record though terminated record for same worker which is updated in the Workday system.
CONCHENAB-2948	Workday aggregation will now work fine even if Past Termination Offset is provided in the application.
CONCHENAB-2951	The Workday Connector now successfully runs delta aggregation following a full aggregation on the same day.
CONCHENAB-2955	The SCIM 2.0 Connector now supports TLS 1.2 while running on IBM WebSphere.

CONCHENAB-2961	The Web Services Connector no longer fails the aggregation and test connection for the applications utilizing Basic Authentication. After upgrading IdentityIQ, the following entry key must be added to the application debug page for the existing applications: <entry key="encrypted" value="accesstoken,refresh_token,oauth_token_info, client_secret,private_key,private_key_password,clientCertificate, clientKeySpec"/>
CONCHENAB-2978	The SCIM 2.0 Connector now does not support ID attribute in patch request for modify operation only.
CONCHENAB-2999	Now provisioning operations work as expected through Cloud Gateway.
CONCHENAB-3090	The SCIM 2.0 Connector now contains group remove attribute for patch JSON request.
CONCHENAB-3093	The SCIM 2.0 Connector now discovers only new schema attribute mappings from target system.
CONCHENAB-3117	The Workday Connector now does not skip worker record terminated on same day.
CONELLIS-1936	The Siebel Connector now supports configurable employment status for enable and disable operations.
CONELLIS-1958	The Duo Connector now uses okhttp-2.7.5.jar and okio-1.15.0.jar to address the security vulnerability issues reported with previous version of these libraries.
CONELLIS-2204	The Delimited File Connector now has the ability to configure a cryptographic algorithm when using SCP.
CONETN-1986	The SAP HR/HCM Connector no longer fails the partitioned aggregation with multiple threads.
CONETN-2127	The Active Directory Connector no longer causes the Identity Request to remain in the ‘Verifying’ state when provisioning a value of accountExpires attribute.
CONETN-2259	The Active Directory Connector no longer causes ConnectorException when previewing accounts for a multi-forested application and lists accounts correctly.
CONETN-2262	The Delimited File Connector now correctly parses the file based on selected parsing type.
CONETN-2327	After upgrading IdentityIQ, the IQService will access only IQService related keys in the registry editor and hence IQService would be installed/uninstalled successfully.
CONETN-2328	The Active Directory Connector no longer causes NullPointerException when running delta aggregation with missing or incorrect user cookies in the application XML. Instead, it will trigger a full aggregation.
CONETN-2337	The SAP Connector no longer causes RfcGetException: Name or password is incorrect (repeat logon) when using After-provisioning rule to assign an entitlement.
CONETN-2342	The TopSecret Mainframe Connector no longer fails when provisioning a default group for a Top Secret account.
CONETN-2343	The Active Directory Connector now no longer fails the aggregation with auto-partitioning and manageRecycleBin options enabled.

CONETN-2345	The IdentityIQ for SAP ERP - SAP Governance Module no longer displays ArrayIndexOutOfBoundsException error when aggregating accounts with a null Contractual User Type ID.
CONETN-2351	The Novell eDirectory LDAP Connector now supports provisioning of entitlements with special characters in the Distinguished Name (DN). To use this functionality, the following keys must be added to the application xml: <entry key="charsToEscapeInDN" value=",+\"<>;"/> <entry key="charsToEscapeAtStartInDN" value="#"/> <entry key="charsToEscapeAtEndInDN" value=" "/> <entry key="charsToEscapeWhileProvisioning" value="/"/>
CONETN-2380	The IdentityIQ for Oracle ERP – PeopleSoft no longer displays java.util.ArrayList cannot be cast to java.lang.String exception when de-provisioning IT Role with multiple entitlements.
CONETN-2383	The ADAM Connector now considers Group Member Search DN attribute of application in account aggregation.
CONETN-2385	The Azure Active Directory Connector no longer supports creating user of type Guest.
CONETN-2390	The Active Directory Connector now has a skipIterateSearchFilterInPTA flag that can be configured to skip or not skip the iterate search filter configured for single search DN during Pass Through Authentication (PTA) for a user.
CONETN-2394	The ServiceNow Connector no longer fails during delta aggregation if a user is modified on the managed system.
CONETN-2400	The LDAP Connector now no longer displays the IQService Host Warnings. The warnings are now only displayed for Active Directory and other connectors that use IQService for provisioning and other transactions.
CONETN-2409	The Azure Active Directory Connector now skips the mail-enabled-security-groups from account group aggregation if skipMailEnabledGroup attribute/flag is set to true.
CONETN-2410	The SAP GRC Application Module now no longer rejects a request containing a provisioning and de-provisioning operation for the same role.
CONETN-2413	The Microsoft SQL Server Connector now displays the date attributes in correct format for all types of accounts.
CONETN-2423	The Active Directory Connector no longer causes NameNotFoundException that occurs due to a collision of Active Directory objects when running delta aggregation.
CONETN-2432	The SAP ERP - SAP Governance Module now no longer displays incorrect warning messages when provisioning or de-provisioning IT roles.
CONETN-2433	The Oracle ERP - Oracle E-Business Suite now no longer fails with a ConnectorException when disabling an account.
CONETN-2441	The Active Directory Connector now builds the Resource Object (RO) with all the available attributes instead of just identity and display attributes when authenticating using Pass Through Authentication (PTA).

CONETN-2447	The JDBC Connector no longer causes Missing IN or OUT parameter at index:: 1 exception when performing Test Connection with a Stored Procedure configured as the SQL Statement.
CONETN-2451	The LDAP Connector now supports aggregating and provisioning a custom group member attribute for posix groups if it is configured as a group schema.
CONETN-2452	The LDAP Connector now retries the aggregation in DEFAULT iterate mode during network connectivity issues.
CONETN-2453	The Mainframe Integration Modules now support the configuration of Pre and Post Scripts return codes from Mainframe Connectors. Customer must add the following entry/entries in the application debug page to support these changes: <entry key="failWhenSkip" value="true/false"/> <entry key="failWhenWarn" value="true/false"/>
CONETN-2454	The IBM Tivoli Directory Server LDAP Connector now supports Unlock Account feature. To enable the Unlock Account feature (featureString: UNLOCK) for an upgraded application, the following attributes must be added to the application debug page: <entry key=""lockAttr"" value=""pwdAccountLockedTime""/> <entry key=""unlockAttr""> <value> <List> <String>pwdFailureTime</String> <String>pwdAccountLockedTime</String> </List> </value> </entry>
CONETN-2459	The Active Directory Connector no longer causes ConnectorException: ObjectNotFound error when provisioning an account or a group using a Load Balancer URL in the Application Configuration.
CONETN-2470	The SAP HR/HCM Connector now no longer causes a GeneralException when a custom rule is configured for the Manager Relationship model.
CONETN-2471	The LDAP Connector no longer causes an error when provisioning an account or a group using a Load Balancer URL in the Application Configuration.
CONETN-2473	The SAP ERP - SAP Governance Module now assigns roles correctly when multiple attribute request with operation as set is present in plan.
CONETN-2476	The ServiceNow Connector now returns the display name or sysid for a schema attribute based on the combination of sysparm_display_value and useSysIdReference configuration parameters in the application.
CONETN-2490	The IBM Lotus Domino Connector now no longer displays the java.lang.NoClassDefFoundError error when creating an application of that type in JBoss 7.

CONETN-2491	The Azure Active Directory Connector has enhanced logging for connection issues in debug mode.
CONETN-2492	The SAP HANA Connector now no longer aggregates and displays as CATALOG_ROLES, the roles granted to a user per schema.
CONETN-2498	The SAP ERP - SAP Governance Module now de-provisions only to be de-provisioned roles.
CONETN-2515	The G Suite Connector now supports provisioning an account with multiple values for aliases attribute.
CONETN-2524	The Workday Connector now successfully provisions an account with a blank attribute value.
CONETN-2529	The IBM Tivoli Directory Server LDAP Connector now no longer abruptly ends the delta aggregation if the last account in a page is out of the scope of the searchDN.
CONETN-2531	The IBM Tivoli Directory Server LDAP Connector no longer causes InvalidNameException when resetting a password for an account with special characters in the Distinguished Name (DN) using self-service password reset.
CONETN-2539	The Active Directory Connector now successfully aggregates the delta account from child domain when delta aggregation is run with iterateSearchFilter.
CONETN-2540	The Microsoft SQL Server Connector now no longer causes InvalidConfigurationException when performing test connection with trailing spaces in the database names listed in the includeDatabases and excludeDatabases fields.
CONETN-2545	The JDBC Connector now no longer displays the column not found exception when column alias is used in the query provided.
CONETN-2550	For Active Directory Connector, the JNDI exceptions are now put at ERROR level for early diagnostics.
CONETN-2552	The Delimited File Connector now executes the pre-iterate rule every time an aggregation is run.
CONETN-2556	For Active Directory Connector, aggregation task will not display the divide by zero arithmetic exception when preloading is enabled.
CONETN-2559	The Oracle ERP – Oracle E-Business Suite now no longer adds a space to description field on password change.
CONETN-2584	The Workday Connector now no longer fails while provisioning a terminated worker having multiple past terminated records.
CONETN-2608	The Active Directory Connector now no longer times out the partitioned aggregation when cache is enabled.
CONETN-2632	The Active Directory Connector now supports provisioning never as a value of the accountExpires attribute for an account.

CONETN-2645	IQService now offers enhanced security of the communication channel between IdentityIQ and IQService using TLS and client authentication. Using this mechanism now all transactions are well authenticated and encrypted. Applications of all connectors that uses IQService now have IQService User and IQService Password fields which are mandatory for IQService configured to communicate over TLS. For enhanced security, this release of IQService now requires Client Authentication to be configured to process any request that it receives on TLS port.
CONHELIX-938	The Epic Healthcare Integration Module now supports WS-Security for common Web Services.
CONHELIX-994	The Epic Healthcare Integration Module now supports AuditUserID for all provisioning operations.
CONHELIX-1009	The Epic Healthcare Integration Module now supports SoftCode endpoints to connect to a native Epic system.
CONHELIX-1014	The Okta Access Management Infrastructure Module now supports List Users with a Filter and List Users with a Search in account management.
CONHELIX-1046	Importing the Epic Healthcare Integration Module configuration as defined in Epic.xml now no longer generates an Unable to deserialize error and now completes successfully.
CONHELIX-1047	The Cerner Healthcare Integration Module now supports Sync Password feature.
CONHELIX-1054	The Cerner Healthcare Integration Module now supports provisioning of multiple Organization groups via a business role.
CONHELIX-1055	The Cerner Healthcare Integration Module now supports Sync Password feature with an authoritative source.
CONHELIX-1139	The Epic Healthcare Integration Module now aggregates LinkedTemplates/SubLinkedTemplates correctly for Account group aggregation.
CONHELIX-1148	The Epic Healthcare Integration Module now aggregates all account groups correctly and no longer terminates account group aggregation abruptly.
CONHELIX-1177	The Epic Healthcare Integration Module with WS-Security configuration no longer supports use of **WS-Policy** and **WS-Security Policy** based configuration. After upgrading to IdentityIQ 8.0, the `epic_security_policy.xml` file must be updated as per the steps provided in the 'IdentityIQ for Epic Healthcare' chapter of the *SailPoint Integration Guide*.
CONHOWRAH-1773	With IdentityIQ 8.0, when groupMembershipSearchDN is not configured then new Active Directory applications will fetch all the group memberships associated with respective account without restricting to defined user's search scope. If desired behavior is to restrict the group memberships for a given account then define the scope under groupMembershipSearchDN.
CONHOWRAH-1778	To enhance the security of IQService against XML external entity attacks, DTD processing in XML parsing objects is now disabled.
CONHOWRAH-1819	IQService now does not print service account password in log file.

CONHOWRAH-1852	The Active Directory Connector no longer fails when provisioning an Integer value for accountExpires attribute.
CONHOWRAH-1917	The Active Directory Connector is now more tolerant to spaces in Distinguished Name during provisioning operations.
CONJUBILEE-55	The Web Services Connector now handles the empty form entries while the body type is selected as Form Data.
CONJUBILEE-85	The Web Services Connector is now capable of excluding request headers from the OAuth2 token generation request.
CONJUBILEE-115	The Web Services Connector now allows to save parameters in application through Web Services Before and After operation rule.
CONJUBILEE-144	The Web Services Connector now handles retry mechanism in create account operation properly.
CONJUBILEE-153	Fixed exception occurring in Web Services connector for Change Password operation when **No Authentication** type selected.
CONJUBILEE-170	The Web Services Connector now supports client certificate authentication in OAuth2 authentication.
CONJUBILEE-184	The Web Services Connector now passes i**nitialised processedResponseObject** argument in After Operation rule.
CONJUBILEE-186	The Cloud Gateway Connector now respects CA certificates and hostname verification during SSL.
CONJUBILEE-204	The Web Services Connector now supports OAuth2 client credentials authentication with Client ID and Client Secret in the request body.
CONJUBILEE-220	The Web Services Connector now supports standard cookies specification for HTTP requests.
CONNAMDANG-1472	The Oracle Database Connector has now been enhanced to whitelist the sub-roles and system privileges before executing the revoke queries to prevent SQL injection attacks.
CONNAMDANG-1734	The DB2 Connector has now been enhanced to not read the native identity attribute from the user schema to prevent the SQL injection attacks.
CONNAMDANG-1736	The DB2 Connector has now been enhanced to whitelist the role name before executing the DROP queries to prevent SQL injection attacks.
CONNAMDANG-1738	The Sybase Connector now supports configuring logical name to connect to the Sybase server.
CONNAMDANG-1747	The DB2 Connector has now been enhanced to whitelist the permissions with respect to the target objects before executing the Revoke queries to prevent SQL injection attacks.
CONNAMDANG-1751	The DB2 Connector has now been enhanced to whitelist the permissions with respect to the target objects before executing the Grant queries to prevent SQL injection attacks.
CONPAMBAN-1525	The Microsoft SharePoint Online Connector now has the default timeout value set to 1 minute (60 seconds). The default timeout is configurable through the application.xml file with the queryTimeout attribute and value in milliseconds.

CONPAMBAN-1642	The RSA Authentication Manager connector now supports version 8.3 and 8.3p1 of RSA Authentication Manager.
CONSEALINK-801	The ServiceNow Service Desk Module update set no longer updates objects which are out of the SailPoint application scope.
CONSEALINK-883	The ServiceNow Connector now no longer fails delta aggregation with com.google.gson.JsonPrimitive cannot be cast to com.google.gson.JsonObject error.
CONSEALINK-886	When an application is configured for ServiceNow Service Desk Module and the Unstructured Target Collector, a service ticket is now generated when the Target Permissions are revoked through a certification.
CONSEALINK-893	The ServiceNow Connector now uses all the cookies received from the response for making subsequent requests for the session.
CONSEALINK-900	The ServiceNow Service Desk Module now correctly displays ServiceNow ticket number in the access request when an Identity has multiple accounts in ServiceNow.
CONSEALINK-934	For ServiceNow Service Desk Module, Incident and Change Request Update Sets have been corrected for the choice action on transform map fields.
CONSEALINK-1052	For ServiceNow Service Desk Module, WSS4J jar would be upgraded from wss4j-1.5.12.jar to wss4j-1.6.19 after upgrade.
CONUMSHIAN-293	In SAP HR/HCM Connector, partitioning aggregation would succeed even if one thread failed.
CONUMSHIAN-2348	In IdentityIQ for Amazon Web Services, PolicyGroups and PolicyRoles are the new attributes that are now available in the default schema of the Customer Managed Policy to allow viewing the list of groups and roles that the customer managed policy is attached to.
CONUMSHIAN-2368	The SAP HR/HCM Connector has an improved account aggregation performance, especially in cases where multiple Action Type is configured.
CONUMSHIAN-2624	The SuccessFactors Connector now displays an appropriate error message when the service account with insufficient permissions or different picklist values are unable to pull in any account.
CONUMSHIAN-2694	The NetSuite Connector has been enhanced to avoid printing secure data during connector logging.
CONUMSHIAN-2751	For IdentityIQ for Amazon Web Services, the dependent third party aws-java-sdk-bundle-1.11.354 jar (which bundles all Amazon Web Services) has been replaced with new custom jar aws-sdk-module-1.0. The new jar bundles the relevant AWS services which the product requires.
CONUMSHIAN-2840	The SuccessFactors Connector is now enhanced with more granular and reduced permission for service account to manage the SuccessFactors Employees and Contingent workers.
IIQCB-2067	The name is truncated when it exceeds the available space. The identity name can no longer exceed the limits of the user interface card boundary.
IIQCB-2086	CPU monitoring is now handled by java 8 APIs. The sigar libraries have been removed from IdentityIQ and are no longer required on the library path of the native operating system.

IIQCB-2092	Text no longer overlaps when resizing the browser window to smaller sizes.
IIQCB-2104	Corrected help text on the **Minimum number of characters** setting in password policy configuration.
IIQCB-2108	Improved the German translation for the **Sign Off Decisions** button.
IIQCB-2110	The branding document has been updated for 7.1+ releases and can be found at: https://community.sailpoint.com/docs/DOC-7952
IIQCB-2225	Updated the Google Apps Getting Started document on Compass.
IIQCB-2233	The SSO Validation rule now runs with every request.
IIQCB-2339	Corrected some issues with French Canadian localization catalog.
IIQCB-2342	Access Request item approval statuses now show correctly regardless of the approvalScheme and approvalMode.
IIQCB-2349	Added localization to an error message related to an unauthorized attempt to access a work item.
IIQCB-2351	The Access Reviews quick link card on the home page now shows the count of active access reviews.
IIQCB-2356	Identity search functions in QuickLink populations uses starts with instead of equals.
IIQCB-2360	**[SECURITY]** The OpenSAML libraries have been updated to mitigate a known External Entity Injection vulnerability.
IIQCB-2386	Improved error handling in the rendering of approval work items. This will decrease the likelihood of the page becoming unusable in a situation where one of many work items encounters an error.
IIQCB-2389	Now when the options to prompt users for unanswered questions is enabled, they will always be taken to the home page after login.
IIQCB-2429	After rotating a keystore, the Encrypted Data Synchronization Task will perform data encryption of domain and forest passwords without requiring a save on the Application Definition page.
IIQCB-2432	Updated The French Canadian translation to address mismatched message keys.
IIQCB-2434	An update has occurred to the sign off message in French Canadian.
IIQCB-2515	The Approvals quick link will be updated to reference the new approvals page introduced with this release. If this quicklink with the name Approvals has been edited to have custom behavior, a new quicklink should be created prior to upgrade so functionality is not overwritten.
IIQHH-567	IdentityIQ has updated to a newer version of log4j. All previously configured logging or other customizations related to log4j.properties must be manually moved to log4j2.properties. The syntax has also changed.
IIQHH-570	A descriptive warning pop up is now displayed if the logged-in user has insufficient permissions to remove access.
IIQHH-571	Filters are now preserved on the Access Request list page after returning from viewing the details of a single Access Request.

IIQHH-575	Implemented changes to approval work items to display the account name for an item whenever it is available.
IIQHH-580	The Advance Analytics now correctly executes searches with collection conditions and OR filters.
IIQHH-664	Corrected Velocity settings to prevent ResourceNotFoundException errors in certain circumstances.
IIQHH-666	Reanimator service no longer terminating queued requests incorrectly.
IIQHH-758	Improved error handling in LCM Provisioning workflow/Access Request user interface.
IIQHH-978	Reports no longer incorrectly terminating when running in a multi-server environment.
IIQKAP-395	Documentation for targeted certifications includes more information about working with rules.
IIQKAP-397	The account mappings section of the SailPoint IdentityIQ Administration Guide contains additional information on extended attribute naming.
IIQKAP-410	Documentation has been updated around the usage of Role Provisioning Policy.
IIQKAP-412	The *SailPoint IdentityIQ Administration Guide* contains additional information about Authentication Method Processing Order and SSO Configuration.
IIQMAG-1922	**Requiring Current Password during the Expired Password Reset** process can be configured on the Passwords tab of Configure IdentityIQ Settings page. This setting defaults to not required during an upgrade, but required for new IdentityIQ 8.0 installations.
IIQMAG-1945	Removal of items is now permitted in access requests that also contain policy violations.
IIQMAG-1947	Performance of the **Completed By** query on the Work Item Archive tab has been improved by converting to the Identity Suggest mechanism.
IIQMAG-1952	Delegated policy violations now show on the Policy Violation List and are accurately reflected in the counts.
IIQMAG-1956	Policy violations involving multiple entitlements and more than one Removal Access Request can now be resolved successfully.
IIQMAG-1967	The Run Rule task now requires a rule argument.
IIQMAG-1969	Exception handling has been refined in the Workflow Library rule to provide more meaningful error information.
IIQMAG-2016	The application name field in Provisioning Policy now behaves properly when there is more than one page of application names from which to select.
IIQMAG-2329	In Access Request approvals, entitlements now display first the Display Name and then the Value field of the entitlement.
IIQPB-760	Accounts that only have targeted permissions no longer display in certifications when the **Include Accounts with no Entitlements** is selected.

IIQPB-768	Workflow splitting for provisioning on approvals now works in cases where account creation is required. All creates targeted to the same application are grouped together unless the plan includes a role with an account selection rule.
IIQPB-781	AccountRequest attributes are now being copied to the compiled integration ProvisioningPlans.
IIQPB-783	When scheduling a targeted certification with the **Exclude Inactive Identities**option, exclusions are no long saved by default. To save exclusion, add the entry includeArchivedIdentities = true to your certDefinition.
IIQPB-788	Made improvements to the algorithm for maintaining Identity Requests for requests for roles with a large number of entitlements. This will improve the performance of updating these requests throughout the request workflow and provisioning process.
IIQPB-789	Made improvements to the algorithm for plan compilation of roles with a large number of entitlements. This increases the performance of Lifecycle Manager Access Request when requesting those roles.
IIQPB-790	Resolved a situation where a permitted role could not be requested through Lifecycle Manager because of improper validation of the role hierarchy. Now correctly flattening the hierarchy to enable requests to proceed as expected.
IIQPB-803	Workflow splitting for provisioning on approvals now works in cases where account creation is required. All creates targeted to the same application are grouped together unless the plan includes a role with an account selection rule.
IIQPB-828	Roles with assignment rules using complex filters are now being assigned correctly when running the Identity Refresh task without the **Refresh Identity Attributes** option selected.
IIQPB-834	Workflow splitting for approval/provisioning now works correctly in scenarios where roles with overlapping entitlements are removed in the same request. An additional check has been added to detect entitlements excluded from all branches of the split.
IIQPB-858	The account selection prompt is performing correctly for permitted roles when there is no ambiguity of the intended target account.
IIQSAW-1304	If you are using the common /rest/suggest endpoints for custom code, you need to add any objects and columns needed to use to the suggestColumnWhitelist and suggestObjectWhitelist configurations.
IIQSAW-1862	SPRights are now more strictly enforced on the Certification Campaigns home page widget. Users with the CertificationAdministrator capability can view, but no longer has the right to edit, certification options.

IIQSAW-1866	Access request approvals now properly prevent the requestor from forwarding the approval.
IIQSAW-1877	The Delimited File Application Status Report no longer supports live preview, and counts are now correct.
IIQSAW-1878	Entries are no longer repeated when a Advanced Analytics Access Request Report is exported.
IIQSAW-1880	Changes to the Account Schema Display Name are now properly updated during aggregation.
IIQSAW-1881	IdentityIQ no longer presents an error during aggregation when an inherited group has been deleted.
IIQSAW-1883	The Entitlement Details dialog is now displaying non-entitlement application attributes when they are part of a role's profile. Additionally, attributes (both entitlement and non-entitlement) are now also displayed when ignoreCase=true.
IIQSAW-1885	**[SECURITY]** Role Editor is no longer accessible to unauthorized identities through a direct link. An error page is displayed if the logged-in user does not have access to Setup->Roles.
IIQSAW-1910	Server Name and Date/Time are now included in thread dumps.
IIQSAW-1970	New configuration option htmlSanitizerPolicies can be modified to enable additional HTML elements for TABLES, LINKS, IMAGES and STYLES.
IIQSAW-1983	**[SECURITY]** Combo boxes in reports are no longer susceptible to content injection.
IIQSAW-1996	Role additions and removals upon the arrival of sunrise and sunset dates are now properly audited.
IIQSAW-2003	Invalid fields in the Forwarding section of the Edit Preferences page are now properly detected and corrections are allowed.
IIQSAW-2015	Richfaces was replaced with Primefaces. Any custom pages that relied on a4j components will need to be updated to instead use an appropriate Primefaces or JSF component.
IIQSAW-2044	Custom AccessRequestTypes now appear in the Access Request list page and in the **Type** filter drop-down.
IIQSAW-2045	In Access Requests, roles and entitlements are now displayed as links for custom IdentityRequest objects types.
IIQSAW-2055	The JSONDeserializerFactory class has been deprecated. The deserialize and deserializeList methods remain, but will only pass through to the JsonHelper. The FlexJSON JSONDeserializer class has also been deprecated. Any custom code or rules should be updated to eliminate any usages of the FlexJSON JSONDeserializer class or the JSONDeserializerFactory class, and instead use the JsonHelper class. All JSON inputs must be properly formed with keys and string values surrounded by either single or double quotes.
IIQSAW-2068	**[SECURITY]** IdentityIQ's SPML Interface has been removed.
IIQSAW-2078	Account Group Membership Certification items targeting identities that are deleted are now shown and can be decided.

IIQSAW-2079	Certification items targeting identities that are deleted are now shown and can be decided.
IIQSAW-2097	**[SECURITY]** A stored XSS vulnerability has been removed for a field in the Application Configuration.
IIQSAW-2105	Customers using WebLogic versions 12.2.1.1 and earlier or JBoss 7.0 and earlier might see errors in the logs regarding failure to parse class files in the log4j-api jar. This is due to the presence of Java 9 classes in the newer log4j jars. Upgrading to WebLogic 12.2.1.2 or JBoss 7.2 resolves the issue.
IIQSAW-2133	**[Security]** A stored XSS vulnerability has been removed for some fields in Role Extended Attribute panels on the Role Management page in the administrator UI.
IIQSAW-2135	Property references to Identity.displayName in the following `UIConfig` file entries will be replaced with parent.targetDisplayName, to avoid unnecessary join. "uiCertificationItemWorksheetColumns", "uiTargetedCertificationItemWorksheetColumns", "uiCertificationItemReturnedItemsColumns", "uiTargetedCertificationItemReturnedItemsColumns", "uiCertificationItemPolicyViolationsColumns"
IIQSAW-2141	If you have Aurora installations you should use the `create_identityiq_tables.mysql` script, first modifying create user section by removing the MySQL section and un-commenting the Aurora section.
IIQSAW-2171	In order to provide better support for upgrading from one plugin version to another, we have enforced some new requirements for plugin version number format. See the "Plugin Versioning Requirements" section of the *SailPoint IdentityIQ Administration Guide* for more information.
IIQSR-35	The number of backgrounded workflows that the System Maintenance task attempted to process is now exposed in the user interface page for the Task Result as Background Workflow Events.
IIQSR-37	Improved performance for the **My Access Review** widget for customers with a lot of access reviews and work items.
IIQSR-39	Certification revocations for IT roles now work correctly when more than one IT role share the same entitlement.
IIQSR-42	A large amount of entitlements granted by a role during its sunrise are now properly stored in the database to prevent an error when the sunrise date is reached and the entitlements are provisioned.
IIQSR-49	Role assignments that create multiple accounts on the same Application now provision correctly.
IIQSR-52	Account details for identity target roles now displays the source role to approve identity warehouse access details.
IIQSR-56	Workflow steps of Approval workItemType now correctly show datatable and text form sections as read-only.

IIQSR-61	If it exists, the application object is now available for use in field validation rules in provisioning forms.
IIQSR-62	If they exist, the link and application objects are now available for use in field validation rules in provisioning forms.
IIQSR-63	A violation pop-up window no longer incorrectly shows for a certification item if the item's role was deleted after the certification was created.
IIQSR-64	The suggest drop-down and search functionality now works correctly for searchable extended attributes of type Identity, in the Entitlement Catalog Advanced Search
IIQSR-68	Exceptions no longer happen in certifications when selecting Details for roles with boolean entitlements or **Account Details** for accounts having boolean entitlements.
IIQSR-69	Identity searches in Advanced Analytics now consider application selections when searching by link attributes.
IIQSR-70	When multiple assignments of the same role are revoked in an access review, they will all be removed rather than only one of the roles associated with the accounts.
IIQSR-72	Temporary identity attributes no longer revert to unchanged values from the feed.
IIQSR-73	The **Tags** drop-down now correctly displays on the Advanced Analytics Access Review search page, when you navigate to an individual access review, and then click the **Refine Search** button to search again.
IIQSR-76	To use additional features, the library commons-beanutils.jar has been upgraded from version 1.6 to version 1.9.3.
IIQSR-77	**[SECURITY]** Resolved an XSS vulnerability in the Role Configuration page and Scopes.
IIQSR-79	Members of workgroups that have special characters in the workgroup name (e.g. '{', '}', '/', ':') can now open workitems assigned to that workgroup.
IIQSR-84	Identity fields in custom forms now allow an empty value, a value is mandatory only when the field is marked as required.
IIQSR-85	Fixed a paging problem when viewing additional access reviews on Microsoft SQL Server.
IIQSR-89	Global Settings for **Email Task Alerts** now work correctly for individual tasks whose **Email Task Alerts** setting is disabled.
IIQSR-90	Special characters [=, +, -, @] can be used as leading characters in PDF, CSF and UI reports, but are still escaped by a single quote to prevent them from being used maliciously in CSV (Excel) reports.
IIQSR-92	Workgroups that are owners of SOD Policy Rules can now be deleted from the debug pages or `iiq console`. This will cause the respective SOD Policy rules that had the workgroup as an owner to have a Policy Violation Owner of None.
IIQSR-94	The **Forgot Password** link on the Login pages is no longer available until the page has finished loading.

IIQSR-95	The Check Expired Work Items task now successfully expires escalated approval work items when appropriate.
IIQSR-96	The Manage Accounts page now correctly handles and displays the canceled state in the Last Action Status column.
IIQSR-99	Title of the Access Review Decision Report is now consistent with the report name.
IIQSR-101	Certification CSV file exports now correctly handle fields with newlines in them.
IIQSR-104	An unstructured target using OAuth authentication in a PAM application can now save a set of credentials separate from OAuth credentials defined in the application configuration.
IIQSR-107	Improved performance and responsiveness in the user interface for users who belong to hundreds of workgroups and are also making an access request.
IIQSR-108	Certification events triggered for an identity without accounts on an included application no longer throw a NullPointerException when the event is processed.
IIQSR-109	If multiple role assignments and multiple accounts are configured on a role that spans multiple applications, then if one or more accounts are deleted natively, reprovisioning missing links for multiple role assignments now creates all accounts instead of only one.
IIQSR-113	Tasks now support scoping. When scoping is enabled, Tasks, task schedules, and results will continue to be available for viewing by their respective owners, but they will now also be available for viewing by users who control the task's assigned scope. Task schedules and task results inherit the Task's Scope setting during the scheduling process.
IIQSR-114	Policy names and policy constraint names and descriptions can contain the ampersand character.
IIQSR-117	Multiple approval comments are no longer compounded in Access Request Status Report when split provisioning is enabled.
IIQSR-119	A CSS file for custom branding now contains the correct formatting so that the background color is not incorrectly overridden in some cases.
IIQSR-123	Duplicate entries are no longer listed in manual remediation work items.
IIQSR-138	Role assignment filters now correctly handle boolean attributes.
IIQSR-144	Archived roles containing entitlements that no longer exist on their newer versions can now be viewed.
IIQSR-145	The Task Results page now correctly displays task results which include Identity data with non-displayable control characters.
IIQSR-146	Corrected issue with pagination being incorrect on object browser in the debug pages for TaskSchedule objects.
IIQSR-149	Filter Identity Selectors in the Role Viewer now display in a more readable form, instead of showing HTML entities.
IIQSR-150	Report definitions without an owner are no longer displayed on the reports tab. All reports must now define `template="true"` to be shown on the Reports tab.

IIQSR-151	Users that have workgroups with System Administrator capabilities can now see the Risk Score widget on the Home page.
IIQSR-152	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.
IIQSR-157	Access Review Decision reports will return the correct results when filtering by tags.
IIQSR-164	The Data Exporter Task now correctly excludes negative role assignments
IIQSR-165	WebService application provisioning failures no longer cause work items created by Provisioning Transaction overrides to not be available for viewing.
IIQSR-167	A thread leak resulting in an OutOfMemoryError no longer occurs when Aggregation tasks are canceled and when aggregating newly provisioned groups from resource objects.
IIQSR-168	Date fields in custom self-service registration forms are now correctly handled.
IIQSR-170	Optimized the query used when viewing Work Item Archives to improve performance on Oracle databases.
IIQSR-190	Email notifications generated by email templates in the Accelerator Pack are now correctly sent, rather than generating a velocity parser exception.
IIQSR-191	The email notification when forwarding an access review work item is now correctly sent out, instead of generating a modulo error from the Velocity parser.
IIQTC-32	Profiles added to a role definition through the user interface will correctly persist special characters rather than them being escaped in the definition of the role.
IIQTC-34	Making self-service requests using an identity with a name containing commas no longer results in errors during policy checking.
IIQTC-36	SSO using SAML now correctly audits logins each time there a new session.
IIQTC-37	Native change detection combined with delta aggregation will correctly reflect the removal of an entitlement from the source application.
IIQTC-38	The **Back** button on access request details now properly redirects you to the previous applicable area, rather than to the Home page.
IIQTC-39	Setting the localUpdate property in a ProvisioningPlan will not cause a concurrent modification error during plan compilation.
IIQTC-40	The sort order on access requests is now properly maintained while navigating to access request details.
IIQTC-41	Performance of the Remove Access tab of the Manage Access area has been improved by factoring out some redundant database queries.
IIQTC-48	A new System Maintenance Pruner task now handles large scale pruning of expired objects.
IIQTC-49	When revoking an item in a Role Composition Certification, the generated workitem will list the removed role only once.
IIQTC-52	Certification details are provided when encountering an error during generation, so that administrators can know which certification generation failed.

IIQTC-55	Clicking multiple times on a single identity in a QuickLink Identity grid will now launch a single workflow only.
IIQTC-56	The **Back** button in Manage Accounts no longer resets the search criteria.
IIQTC-57	Search suggestions no longer include entries not allowed by a Quicklink configuration.
IIQTC-58	Account revocations are properly displayed only once per account in a remediation work item, instead of multiple times.
IIQTC-6	The target attribute value of a required IT role shared by more than one business role will now be correctly provisioned to the linked application account during an Identity Refresh with **Provision Assignments** selected.
IIQTC-60	A role with condition ISNULL in a entitlement no longer causes a NullPointerException when running a certification.
IIQTC-63	Identities selected in previous quicklinks will be cleared when selecting the next quicklink.
IIQTC-65	Using the **Back** button in multiple areas of the user interface now properly redirects the user to the previous applicable area.
IIQTC-66	Duplicate items in bulk reassignment requests no longer cause errors.
IIQTC-67	The user interface for saving the SMTP server password will correctly save if the password confirmation is correct, rather than always indicating an unmatched password.
IIQTC-71	Application forms to change the password now display the correct fields.
IIQTC-72	Overlapping provisioning policy fields between a role and application no longer results in duplicate provisioning forms.
IIQTC-74	Plan arguments are now merged appropriately when existing attribute assignments are present.
IIQTC-77	Roles and entitlements that have pending remove requests can no longer be selected to be removed again through Manage Access in the LCM.
IIQTC-83	The paging control on the Inherited Roles page now shows the correct number of pages when switching between the definition of different roles.
IIQTC-85	**[SECURITY]** The error page is no longer susceptible to content injection.
IIQTC-87	Rule-based role assignments modified and changed using role change propagation no longer change the source from rule to RolePropagator.
IIQTC-94	The Perform Maintenance task no longer ignores backgrounded-approval-completion items that have expiration dates.
IIQTC-99	Roles in multiples of 10 can be added successfully to an identity.
IIQTC-101	The filters available in the Access request feature have been revised to apply the correct scoping. This action ensures that the user interface will display the correct suggested resources.
IIQTC-108	Assigned roles with the same assignment id are now given separate identity entitlements and displayed correctly in the View Identity Access page.

IIQTC-117	Role targets are no longer removed when updating the sunset date through an LCM request.
IIQTC-119	Manual work items without a workflow case can now be archived, depending on system configuration.
IIQTC-132	Executing an Identity search in Advanced Analytics prior to an Entitlement Analysis search now completes successfully.
IIQTC-135	Applications in maintenance mode where retry is allowed no longer produce errors within Identity Requests.
IIQTC-136	The DataExport task is now able to export table DDLs when executing from a .WAR file.
IIQTC-137	Multivalued fields of type string with an AllowedValuesDefinition on a custom form will not lose their display value on postBack.
IIQTC-138	If there are more than 5 attributes to show in the entitlement attribute drop-down list, a **Load more** button is displayed to show all attributes.
IIQTC-144	Access request approval comments containing special characters are now displayed properly in the user interface.
IIQTC-146	Rapidly launching the same workflow many times will not cause SQL errors when the resulting task results have the same name.
IIQTC-148	Certification items upon which a remediation has been performed prior to the certification completion are now marked as No Action Required for remediation action rather than openWorkItem.
IIQTC-150	This field is required will only display once in forms.
IIQTC-152	Snapshot isolation in SQL Server now is enabled by default in the database upgrade scripts, which matches the database creation scripts.
IIQTC-153	When policy violations are encountered in Access Request, the **Previous** button is disabled.
IIQTC-159	The Access Review Decision Report correctly filters on application and managers.
IIQTC-161	Only configured Identity attributes will trigger related audit events.
IIQTC-167	Batch request items are no longer orphaned when the batch request is deleted in the user interface.
IIQTC-175	Unicode characters are now properly displayed in user-input fields.
IIQTC-177	Search Reports that have a lot of fields to display and data containing tabs can be exported to PDF and CSV successfully.
IIQTC-178	SSO using SAML now correctly audits logins each time there a new session.
IIQTC-183	The Entitlement Owner Access Review Live Report now displays the account name for excluded items.
IIQTC-180	Modifying a ColumnConfig in the uiWorkitemListCardColumns entry in the UIConfig that uses the created date will be reflected in the user interface. This applies to the cards in My Work -> Work Items.
IIQTC-185	Unicode characters are now properly displayed in user-input fields.

IIQTC-213	The extended identity attributes specific to the Accelerator Pack were updated to maintain compatibility with IdentityIQ.