IdentityIQ Release Notes

These are the release notes for SailPoint IdentityIQ, version 6.4

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:

- New features – enhancements and features added since the last release
- Special Upgrade Considerations – specific guidelines for various configurations
- Supported Platforms – supported platforms, environments and applications
- Resolved issues – resolved problems in this release
- Known issues – known problems in this release and ways to avoid them

SailPoint IdentityIQ 6.4 Overview

IdentityIQ 6.4 provides new features and capabilities across the product, including Compliance Manager, Lifecycle Manager, the Governance Platform and connectivity and integrations. Key enhancements in the release include:

- Extended Responsive Mobile User Experience
  - New self-service access request and delegated access request user interfaces that are mobile enabled allow users to request access on the go.
- Role propagation to Role Members
  - Role administrators can now make changes to role definition within the role management user interface and have those changes propagate to assigned members reducing the time it takes to get identities the correct access.
- New Extended Application Schema Model Support
  - Model applications with greater flexibility by creating more than one group type object to represent objects that are critical to applications.
  - Support is added by connector and includes: Oracle EBS, JDBC, Delimited File, SQL Loader.

- Form Editor Updates
  - IdentityIQ administrators now have a centralized form view for forms and can reference standalone forms across the product.
- Cross-Authorization Permission Remediation
  - Automate the remediation of permissions from group permission certifications when a permission resides on a different system.
- Expanded Connectivity and Integration Support
  - New Service Desk Integration for HP Service Manager
  - New Integration with Lieberman Enterprise Random Password Manager (ERPM)
  - Support for effective permissions for SharePoint and Windows File share
  - Support for automated data export task for HP ArcSight integration
  - Connector updates and additions to the following: Active Directory, Oracle HRMS. PeopleSoft HRMS, Salesforce, Oracle DB, Oracle EBS, JDBC, Delimited File, SQL Loader, and Duo Security

IdentityIQ Feature Updates

Extended Responsive Mobile User Experience

IdentityIQ 6.4 introduces two brand new user interfaces that were built from the ground up to function on different device types. The supported interfaces are:

- Self-Service Access Request
- Delegated Access Request

Feature / Enhancement	Description	Benefit
Mobile Ready: Self-Service Access request	A new user experience focused on delivering self-service access request using a mobile device. Users can now request access and go through a regular request flow that includes commenting on requests and specifying a sunrise and sunset date.	Offers users more flexibility to request access while on the go.
Mobile Ready: Delegated Access Request	A new user experience focused on delivering delegated access request using a mobile device. Users can now request access for others and go through a regular request flow that includes commenting on requests and specifying a sunrise and sunset date.	Enables managers and other delegated user types to request access on behalf of others while on the go. Streamlines the correct access to the correct people.

Role Propagation to Role Members

IdentityIQ 6.4 adds new support to its role model with the introduction of role propagation. The feature enables administrators configuring steps in the environment to automate the propagation of role model updates to assigned members without having to make manual changes.

Feature / Enhancement	Description	Benefit
Automated role propagation changes	Enable users to update role definition within the user interface and then automatically propagate changes to every impacted identity. This includes entitlements changes, inheritance and the removal of roles.	Makes role management easier by reducing the time it takes to sync actual state with desired state as changes are made automatically without manual interventions.
Role propagation task	New task that will propagate role changes. For each event it will identify impacted identities and propagate the changes to them.	Provides IdentityIQ administrators flexibility in managing the impacts of changes within the environment.

New Extended Application Schema Model Support

IdentityIQ 6.4 introduces extended application schema support that extends the governance footprint and enable deeper modeling of applications and associated relationships between accounts and other object within a target system.

Feature / Enhancement	Description	Benefit
Define additional application schema objects	The ability to define multiple application schema objects and create relationships between them and account level schemas.	Provides greater flexibility to administrators when defining an application within IdentityIQ so they can provide greater visibility and controls for a target system.
Entitlement catalog updates	The entitlement catalog interface now supports the ability to see application level object relationships and actually add and removes these relationships.	Provides IdentityIQ administrators with greater control over entitlements and provides a way for them to manage entitlements directly within IdentityIQ instead of the native system.
Connectors that support this model	Oracle EBS JDBC Delimited File SQL Loader	Specific connectors that enable the use of the above features.

Form Editor Updates

IdentityIQ 6.4 introduces a number of updates to the form editor that make it easier to create and maintain forms for improved deployment and ongoing maintenance.

Feature / Enhancement	Description	Benefit
Centralized location of form editor	Enables administrators to view all forms from a central location as well as create a standalone form.	Reduces time to find and create forms.
Reference forms	Enables administrators to have the ability to create a form that can be referenced as part of provisioning policies, role policies and workflow forms.	Simplifies form management by increasing administrative efficiency.

Cross Authorization Remediation Support

IdentityIQ 6.4 adds upon flexibility introduced in version 6.3 for automating the removal of permission from a group permission certification to also include cross application remediation. For example, permissions that reside on a different system such as a SharePoint permission on an Active Directory group can now be removed automatically without the need for manual change.

Feature / Enhancement	Description	Benefit
Automate the removal of permissions that reside on different system	Group permission certifications now support the automated removal of permissions when the source of the permission can reside on a different system. For example: the review of and Active Directory group that has SharePoint permission assigned to it.	Automated certification remediation eliminates potential for error and reduces the time it takes to complete the change.
Dual channel unstructured target support	Unstructured target collections now support the ability to define a read source to pull in permissions and then specify a different write channel so that out of the box connectors can be used.	Provides administrators with greater flexibility to put controls in places without having to change their internal environments.

Additional Enhancements

Compliance Manager

Feature/Enhancement	Description	Benefit
Limit the number of reassignments in access reviews	Limit the number of reassignments that can occur in a certification campaign. Administrators can specify the number of reassignments allowed at a global or per certification level.	Reduce security risk and potential audit deficiency.

Lifecycle Manager

Feature/Enhancement	Description	Benefit
Force the removal of assigned entitlements when removing detected roles	New configurable option that forces the removal of any underlying assigned entitlements when attempting to remove a detected role.	Forces the removal of access so that access does not remain if a user has requested it be removed.
Persist password data as a one way hash	New configurable option that will persist password data as a one-way hash replacing two-way encryption.	Improves the security of storing passwords within IdentityIQ.

Governance Platform

Feature/Enhancement	Description	Benefit
Debug Object Editor	Debug pages now include text highlighting.	Makes it easier for administrators to write code with fewer syntax errors.
Delete Account Threshold	Account aggregations now includes a delete threshold which can be set up to send a warning if the threshold Is met.	Provide visibility and pro-active warning to administrators to prevent changes from occurring in the system that could cause major issues.

Connectivity and Integration Enhancements

Service Desk Integration with HP Service Manager

IdentityIQ 6.4 now supports HP Service Manager as an additional Service Desk platform for fulfillment.

Feature / Enhancement	Description	Benefit
Create incidents and change Requests	An IdentityIQ provisioning action triggers incident or change requests to be created in HP Service Manager.	Increases Helpdesk productivity with the direct assignment of incidents/change requests to the Helpdesk for the provisioning operations performed in IdentityIQ.
Track incidents and change requests	The status of the created incident/change request is updated in the respective IdentityIQ access request.	Provides required visibility of the provisioning requests to managers, users, and the Helpdesk.

This integration is licensed as part of the SailPoint IT Service Desk Integration Module.

Integration with Lieberman Enterprise Random Password Manager

IdentityIQ 6.4 introduces privileged account management integration with Lieberman Enterprise Random Password Manager (ERPM). Using this integration the granular level privileges assigned to users on ERPM Management Sets can be reviewed and remediated.

Feature/Enhancement	Description	Benefit
Aggregation of permissions	The ERPM permissions assigned to ERPM users and groups are aggregated.	Visibility into the privileged users and the permissions assigned to them.
Manage ERPM Permissions assigned to Management Sets	The permissions assigned to Management Sets in ERPM are associated with respective users and groups in IdentityIQ.	Help enterprises meet regulatory compliance and security objectives as Access Review and Remediation for privileged users can now be performed.

Lieberman ERPM integration is licensed as part of the SailPoint IdentityIQ IT Security Integration Module.

HP ArcSight Integration Update

IdentityIQ 6.4 simplifies the mechanism to export the identity context and audit data from IdentityIQ to HP ArcSight.

Feature/Enhancement	Description	Benefit
Data Export	A new task ArcSight Data Export has been introduced. It copies IdentityIQ audit and identity context data from IdentityIQ database tables into separate tables designed for HP ArcSight.	Increase enterprise security as ArcSight administrators can configure security rules and generate security alerts based on this data.

Feature/Enhancement	Description	Benefit
Associate an IdentityIQ application name with HP ArcSight source	IdentityIQ administrators can use the ArcSight source names and map those to IdentityIQ applications.	Reduce the risk of error as ArcSight administrators can easily associate an entitlements with ArcSight source.

New Connectors

IdentityIQ 6.4 delivers new out-of-the-box connectors for enterprise and SaaS applications which simplify connectivity to these systems.

Feature/Enhancement	Description	Benefit
New SaaS connectors	Duo Security	Enables integration with target systems for access certification and user provisioning operations.
New Enterprise connectors	Oracle E-Business	Enables integration with target systems for access certification, password management and user provisioning operations. Support for Oracle E-Business roles and responsibilities by leveraging the IdentityIQ extended application schema feature introduced in v6.4.

Active Directory Connector Updates

IdentityIQ 6.4 improves the support for the Active Directory connector.

Feature/Enhancement	Description	Benefit
User Interface for Active Directory application	Configure Active Directory multiple domains using the Active Directory application configuration interface.	Simplifies and reduces the risk of errors while configuring an Active Directory application.
Support for Active Directory domain discovery	Discover Active Directory domains using the Active Directory Global Catalog.	Reduces the time it takes to configure an Active Directory forest environment and the individual domains within it.

Upgrade Consideration: Customers are required to upgrade to v6.4 of the IQService to use the IdentityIQ 6.4 Active Directory connector.

IdentityIQ Cloud Gateway Updates

IdentityIQ 6.4 supports the following features for Cloud Gateway:

Feature/Enhancement	Description	Benefit
Support for partitioning	The Cloud Gateway can perform aggregation based on the partitions defined in an application.	Improved performance during aggregation.
Support for delta aggregation	The Cloud Gateway can aggregate only the changes done on the target system.	Improved performance during aggregation.

Enhanced Connectors and Integrations

IdentityIQ 6.4 also provides updates to a number of existing connectors and integrations to support expanded use cases and new versions of target systems.

Feature/Enhancement	Description	Benefit
Support for ProxyHost and ProxyPort - BOX - Google Apps - AWS - AirWatch MIM - MobileIron MIM - Yammer	proxyHost and proxyPort settings can be specified for these applications.	Increase security and meet internal security policies by installing IdentityIQ behind a proxy server.
StealthAUDIT SharePoint and Windows Fileshare Target Collectors	Support for effective permissions.	Increased security as direct as well as indirect permissions assigned to users can be reviewed, and remediated (through workitems).
Forefront Identity Manager Provisioning Integration Module (FIM PIM)	Support for Forefront Identity Manager Web Portal and Forefront Identity Manager Sync Service to be on different hosts. Support for UserPrincipalName (UPN).	Increased alignment to FIM deployment best practices.
PeopleSoft HRMS and Oracle HRMS Connectors	Ability to write back phone and e-mail updates to the application.	Increased productivity for HR as HR can now enable end users to update specific attributes.
SAP Connector	Support for direct SAP Roles.	Accurate representation of user entitlements as only the direct roles assigned to the user are reported as entitlements.

Feature/Enhancement	Description	Benefit
Salesforce connector	Support for PermissionSet.	Increased security as Salesforce PermissionSet can now be included in Access Review and remediation, Increased productivity as users (self-request) / managers (request for others) can themselves request for Salesforce PermissionSet.
Oracle DB Connector	Support for SYSDBA and SYSOPER privileges.	Increased security, as system level privileges can now be part of access review.
IQService	Size based rolling of logs.	Ease of analyzing the IQService logs with reduced file size. Increased availability of the IQService host as the drive on the IQService host will not fill up now.
LDAP	Support for Account Group Membership Iterate Filter.	Improved visibility into entitlements by filtering only those entitlements as relevant for the business.
Lotus Domino Connector	Support for attaching ID file to mail file on change password	A Lotus Notes user can access his e-mail with the new password.

Platform and Language Updates

Component	New Version
Web Browser	Microsoft Internet Explorer 11, Firefox ESR 31
Mobile Web Browsers	Android 4.4 on Chrome, iOS 8.1 Using Safari, Windows 8 .1 using Internet explorer
Application Servers	JBoss Application Server 7.2 and 7.3
Databases	Microsoft SQL Server 2014
Operating Systems	Microsoft Windows Server 2012 R2
Languages	Simplified Chinese

Component	New Version
Connectors	Oracle DB Connector - Support for Oracle 12c (non CBD) LDAP Connector - Support for OpenLDAP 2.4.39 RSA Connector - Support for RSA Authentication Manager 8.1 PeopleSoft Connector - Support for PeopleTools 8.54 Linux Connector - Support for RHEL 5.11, RHEL 6.5, RHEL 6.6, RHEL 7.0, SUSE Linux, and Enterprise Server 12

Important Upgrade Considerations

IdentityIQ 6.4 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.

Upgrade Processing Time

One of the upgraders is the equivalent of an Identity Refresh and is configured out of the box to use five threads. This configuration is not sensitive to the number of processing cores available, but is controlled through configuration in `WEB-INF/config/upgrade.xml`. Do not increase this number beyond 1.5-2 times the number of processing cores or you will starve threads as they wait for CPU time and the upgrade process will take longer than if a single thread were used.

This upgrader was included in 6.3p1 and later 6.3 patches and will not run again if it has already been run in your environment.

Object Model Upgrade

The upgrade process will modify some of the IdentityIQ configuration objects. If XML representations of these objects are contained 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
  - Due to increased support for Active Directory multi-domain forests and use of multiple Active Directory servers, the configuration structure of the connectivity information has changed. The upgrade will convert the application definition to the new format, but use of an application in the old format will fail.
  - Provisioning and aggregation related feature strings for applications as well as group hierarchy definition have been moved from the application to the specific schema inside of the application. Any attribute in the account schema that is marked as a group attribute will have its type changed to the group schema object type.
  - A new Profiles schema is added to any AirWatch Mobile Device Management applications.
  - The feature string SHAREPOlNT_TARGET is updated to UNSTRUCTURED_TARGET in SharePoint applications.
- TaskDefinition
  - The refreshLinks argument is removed from any instances of the Refresh Logical Accounts task. This functionality has been removed from the user interface to prevent use of the often unnecessary and very resource expensive processing it enables.
- Form
  - Forms of type Report and WorkflowConfig have been marked as hidden to prevent their visibility in the new Form Editor.
- SystemConfiguration
  - The path for the location of the Lifecycle Manager Full Text lndex has been moved from a FullTextIndex object to an attribute in the SystemConfiguration.
  - The SystemConfiguration attribute checCaseSensitive has been changed to be correctly spelled checkCaseSensitive

Active Directory Applications

The application attribute model for storing connectivity and search information for Active Directory domains has changed to further support multiple domains, multiple servers, and Active Directory forest environments. The 6.4 upgrade process will update the configuration in existing applications, so there is a strong requirement to export the updated configuration to replace any XML representations of Active Directory application persisted externally. An application from an installation prior to 6.3 that is imported into 6.4 will not work unless the upgrade process is re-run.

All instances of lQService must be updated to match the ldentitylQ server version.

Full Text Search

Full text indexing of role and entitlement data is now enabled by default for new installations where Lifecycle Manager is enabled (upgraded installations will retain their existing configuration). This allows searching during access request across name, description, and other configurable data stored on roles and entitlements. lndexes are now created using the Full Text Service which allows indexes to be created on all ldentitylQ cluster servers. ldentitylQ will need a writable directory to create the indexes, and the default value is the WEB-lNF directory in the application root. lndexes are refreshed every hour by default. Configuration is available in the Additional Options section of Lifecycle Manager Configuration.

Connectivity

Connectivity is critical to successful lAM deployments. SailPoint is committed to providing design, configuration, troubleshooting, and best practice information to deploy and maintain connectivity to target systems. SailPoint has modified the structure of the Direct Connectors Admin and Config Guide to aid customers and partner deployments. For more details on design, troubleshooting and deployment best practices, refer to the Connector and lntegration Deployment Center in Compass.

BMC Identity Management Suite

Due to the end of life of BMC ldentity Management Suite, the BMC ldentity Management Suite Provisioning lntegration Module is no longer supported.

Architectural Changes

Application Multiple Group Support

To support management of applications that have multiple grouping constructs, ldentitylQ will now support multiple group object types for an application. This support is dependent on support provided by the connector implementation. ln this release, the Oracle E-Business, JDBC, Delimited File, and SQL Loader connectors have this support.

Application attributes that previously used the group. prefix will now use the object type defined in the application's group schema as the prefix. While not required, best practices dictate picking an object type name that does not contain a space.

Schema attributes that are values for another object type, must set that object type as the schema attribute type. For example, the values of memberOf in Active Directory are the objects in the group schema, so the memberOf attribute type should be group and not string.

ManagedAttribute objects will also use the schema object type as the type.

Account Group Aggregation will aggregate all group object types on an application unless the task is configured to exclude certain object types.

Tables that allow viewing account groups will also include a column for the object type. Similarly, filtering and searching for account groups will allow specifying the object type.

Custom code and rules must be changed to understand that there may be more than one group type on an application.

Hashed Sensitive Data

All ldentitylQ data that does not require two-way encryption can now be hashed instead of encrypted. This is a one-way algorithm that prevents obtaining the original clear text value. Any custom code or rules that interact with encrypted data will need to use the new service APl class sailpoint.api.EncodingUtil. Methods are available to encrypt data and check for a match to previously encrypted or hashed data. Please consult the JavaDoc provided with the product for additional details.

Hashing must be explicitly enabled in the Passwords section of the ldentitylQ Configuration page. The Encrypted Data Synchronization Task can be used to convert sensitive data to hashed format.

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.

API Changes

sailpoint.object.IdentityRequest

The previously misspelled isSucessfull method in sailpoint.object.IdentityRequest is now correctly spelled isSuccessfull.

saipoint.object.ManagedAttribute

The group attribute has been deprecated.

Automated Permissions Provisioning

If automated permissions provisioning is desired for permissions aggregated target collectors, the NO_PERMISSIONS_PROVISIONING and NO_GROUP_PERMISSIONS_PROVISIONING feature strings need to be removed from the application.

Mainframe Connector Permissions

Permissions aggregated from mainframe connectors are now in a new more readable format. This format is expected when provisioning operations that reference these permissions are sent to the connector. Because of this, all certifications and active access requests that contain permissions from mainframe connectors should be completed prior to upgrading to 6.4.

Role and Entitlement Assignment

When a role assigned to an identity is removed, if the role contains account attributes that were explicitly assigned to the identity, the entitlement and the entitlement assignment will now be removed from identity. Two new SystemConfiguration options, retainAssignedEntitlementsDetectedRole and retainAssignedEntitlementsAssignedRole are available to restore previous behavior.

Forms

Form fields that reference an attribute name containing a period must enclose the period in quotes. For example, "INFO.ACID_SIZE".

Supported Platforms

Operating Systems

- lBM AlX 6.1 and 7.1
- Red Hat Enterprise Linux 5 and 6
- SuSE Linux Enterprise Server 10 and 11
- Solaris 10 and 11
- Windows Server 2008 R2, 2012, and 2012 R2.

Databases

- lBM DB2 9.7 and 10.5

  Note: IdentityIQ does not include the JDBC driver for lBM DB2. You must obtain the driver directly from lBM.

- MySQL 5.5 and 5.6
- Microsoft SQL Server 2008 R2 and 2012
- Oracle 11g R1, R2, and 12c

  Note: IdentityIQ includes the latest Oracle Database and SQL Server JDBC drivers at the time of the IdentityIQ release. Vendor documentation for the included JDBC drivers indicates compatibility across database server versions, but experience has shown some incompatibilities. You should obtain the latest database server version-specific JDBC driver from your database server vendor.

Application Servers

Note: JDK 6, JDK 7, and JDK 8 are supported as required by the specific application server.

- Apache Tomcat 6.0, 7.0
- Oracle WebLogic 11g (10.3.x) and 12c
- lBM WebSphere 8.0 and 8.5.x
- JBoss Application Server 7.3 and 7.4 (included with Enterprise Application Platform 6.2 and 6.3)

Java Platform

- Sun, Oracle or lBM JDK 6, 7 and 8
- Oracle JRockit JDK for Java version 6

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.

- Firefox ESR v.31
- Google Chrome 30+
- Windows lnternet Explorer 9, 10, and 11

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.

- Safari 7

Mobile User Interface OS/Browser Support

- Android 4.3 and 4.4 on Chrome
- iOS 8.1 using Safari
- Windows 8.1 using Internet Explorer
- Native Browser Blackberry 10.2

Languages

- Brazilian Portuguese
- Dutch
- English
- French
- German
- Italian
- Spanish
- Simplified Chinese

Resolved Issues

(ETN:16701) When a user has SSO enabled and the **Prompt users for answers to unanswered authentication questions upon successful login** option is select, the user is now redirected to answer authentication questions when accessing IdentityIQ pages through SSO authentication.
(ETN:17137) The Identity Refresh task is now more tolerant of incompletely defined role profiles.
(ETN:18330) The persistence model of results from partitioned tasks was changed to prevent undesired performance degradation for tasks with a large quantity of partitions.
(ETN:18339) The size of the constraintName fields in MitigationExpiration and IdentityHistoryItem objects is increased to allow larger names.
(ETN:18380) The 'isAdvance' attribute introduced in 6.2 for JDBC applications has been removed to prevent confusion related to row merging during aggregation.
(ETN:18734) Provisioning a new account on an application with an existing account will now update the correct persisted account after provisioning is complete.
(ETN:18792) Results from modifying an advanced analytics search will now display the first page of results and will no longer fail if the second result set has fewer pages than the first.
(ETN:18796) Identity Refresh is now more tolerant of an empty attribute value in a multi-valued account attribute.
(ETN:18907) Changes to email recipients during configuration of a certification will no longer inadvertently modify the selected email template.

(ETN:18990) PDF export of reports with no data now contain the report outline instead of blank pages.
(ETN:19100) Inline scripts for role assignment are now thread safe and can be used in multi-threaded Identity Refresh.
(ETN:19143) IdentitySnapshot now contains assigned roles which enables certifications to show Changes Detected for assigned roles.
(ETN:19162) The informational message that displays if you make an access request that will result in a policy violation and you have disabled the **Allow Requests with Violations**, will now clearly indicate the allowable actions.
(ETN:19297) The Value column in the Direct Entitlements table of the role modeler is now sortable.
(ETN:19380) Refresh tasks can now take additional parameters to change the way that events are processed to reduce or eliminate the possibility of getting an ObjectAlreadyLocked exception.
(ETN:19438) The Define Identities table display performance can now be improved by disabling the filter of workgroups.
(ETN:19479) Browser timezone calculation is now correct when SAML-based authentication is enabled.
(ETN:19545) Lifecycle Manager object request authority rules are now persisted with name references instead of object ids to enable configuration portability between environments.
(ETN:19727) Approval items now contain displayablename and owner attributes for possible use in notification email templates.
(ETN:19728) Disabled Identity Triggers are no longer used during native change detection.
(ETN:19800) Batch requests to add a role to an identity with a sunset date in the past will no longer have the role assigned.
(ETN:19954) Role removal requests in Lifecycle Manager will now show the owner of the role in the Review and Submit summary page.
(ETN:19980) Entitlement descriptions detected as containing HTML that is not valid will now be correctly filtered for safe and permitted HTML. This allows characters such as < and > to be used without being escaped.
(ETN:20003) Errors generated during Self-Service Registration are now displayed to the user.
(ETN:20132) Aggregation can now be configured to not perform identity attribute promotion using the noAttributePromotion Aggregation task variable.
(ETN:20333) A task schedule with a frequency of Daily can now be correctly re-scheduled by changing the next execution time.
(ETN:20411) Identity Refresh will now log an informative message when refreshing an identity with an account for an application that does not have an application schema defined.
(ETN:20435) Implicit approvals where the requester is the approver are now audited and tracked in the Identity Request object.
(ETN:20465) Form field values in sections that can be hidden are now processed correctly.
(ETN:20517) The details for a policy rule will now adhere to the renderer configured for the policy in the detail view of an access review. This is accessed by clicking on the rule name when viewing the details of an identity in an access review.

(ETN:20667) A password reset request using Forgot Password can now be treated as a self-service password change for Active Directory on Windows Server 2008 R2 and later and have Active Directory password complexity and password history policies validated.
(ETN:20698) The progress bar graphic in certifications that are complete because there are no items will now be displayed correctly to represent 100% complete.
(ETN:20746) Attributes consisting of lists of permissions will now be displayed correctly within the Identity History and Certification Snapshots sections of the History tab of the View Identity page.
(ETN:20753) Workgroup assigned capabilities are now used when determining access to archived work items.
(ETN:20766) Improved performance of removing account groups detected as deleted in the managed system during aggregation for multiplexed connectors with large numbers of multiplexed applications.
(ETN:20799) Escalation email notification to workgroups without an email address and configured to send email to members will now be sent correctly.
(ETN:20800) Cursor focus is now handled correction for wizard forms with postback enabled.
(ETN:20834) Validation checks for duplicating authentication question answers are now case insensitive.
(ETN:20835) Identity selection in custom forms with multiple identities with the same display name now correctly select the correct identity when cursor focus is changed from the identity select box prior to submission.
(ETN:20856) The BMC ESS provisioning integration module will now properly process a provisioning plan with multiple account requests for different ESS persons.
(ETN:20865) Items can now be deleted from multi-value text boxes in custom forms.
(ETN:20891) Implicit approval of work items where the requester is the approver will now work if the approver is a workgroup and the requester is a member of that workgroup.
(ETN:20898) Improved performance when searching populations for entitlements when requesting access in Lifecycle Manager.
(ETN:20903) Correctly show an empty label for a policy violation without a description when revoking a policy violation and displaying the policy violation details.
(ETN:20905) Forwarding of access reviews from the Access Review Search and Monitor->Certification pages is now disallowed when the certifications have multiple certifiers. However, the certifiers can still forward their own access reviews from the Manage->Work Items page.
(ETN:20922) Using the browser back button in Internet Explorer 8 from the dashboard, after login will no longer cause the browser to enter an infinite redirect loop.
(ETN:20927) Prevent prompting for attribute values using unanswered questions when a provisioning plan already has a value and required is set to true.
(ETN:20931) Identities other than those presented in an identity selection field can no longer be manually entered.
(ETN:20977) Identity Refresh will no longer fail when processing a policy violation for an identity that does not have an owner.
(ETN:20987) The application and instance fields are consistently shown on the Audit and Access Request Advanced Analytics search panels, regardless of the order in which the panels are navigated.
(ETN:21023) The narrow results tab in Lifecycle Manager access request will now display properly in low resolution environments.

(ETN:21034) New policy violations now reflect the current decision status in the policy violation detail view instead of the status of a decision on a previous instance of the policy violation.
(ETN:21094) Password history will now be validated in Lifecycle Manager when **Select Synchronize passwords for selected accounts** is active.
(ETN:21153) An application can now be edited when an account extended attribute with a named column name and an associated icon configuration is defined.
(ETN:21198) The SQL Server connector will now process SQL Server role removal requests correctly.
(ETN:21234) Comments made when forwarding a workitem are now available within the workitem forwarding rule.
(ETN:21238) Lifecycle Manager access requests with sunrise/sunset dates are now properly merged into existing pending operations from a previous access request so that pending operations are not lost.
(ETN:21240) Multi-valued report attributes are now correctly made available to the report implementation preventing cast exceptions when a report is run.
(ETN:21257) Dynamic date ranges now display correctly when editing time periods of an active certification.
(ETN:21287) The previous advanced search filters are properly restored when returning from viewing access request details in the Manage Access Requests page.
(ETN:21295) Provisioning requests made through legacy lntegrationConfigs are no longer made on each identity refresh when one is already pending.
(ETN:21296) Changes to workgroup capabilities are now audited when capability auditing is enabled.
(ETN:21297) Access Review filter options are now localized.
(ETN:21307) The processing for a certification when it is complete will now tolerate a mitigator that no longer exists in the system by selecting the certifier, the certification owner, or the default system administrator.
(ETN:21318) Lifecycle Manager will now allow filtering on applications that have a + in the name.
(ETN:21319) SharePoint target collection now uses paging to enable reading large datasets. The page size is configurable using the TargetSource attribute named pageSize.
(ETN:21339) The work item **Complete** and **Save** buttons are now re-enabled when canceling an electronic signature sign-off.
(ETN:21346) The display name for an entitlement is used more consistently throughout the product instead of the entitlement value.
(ETN:21347) Narrowing results in Lifecycle Manager access requests now works when full text indexing is enabled.
(ETN:21353) The status of Lifecycle Manager requests now has an initial value of Pending, will show a status of lncomplete immediately if any of the individual provisioning requests has a failure, and will show a status of Success if all provisioning completes successfully.
(ETN:21379) The identity suggest component will now support an apostrophe in the identity display name.
(ETN:21381) When **Allow requesting additional accounts** is enabled, account selection will now be enabled for permitted roles.

(ETN:21386) Passwords that start with a number and have a colon in their clear text form are now supported across the product as long as they are less than 26 characters. Otherwise, it will be assumed that the password is in its encrypted form.
(ETN:21397) The workgroup member fields to display on the workgroup tab can be specified in the UlConfig for workgroupMemberColumns.
(ETN:21415) Identity suggest components will now allow a search filter with a space to match an identity name that contains a space.
(ETN:21416) The Encrypted Data Synchronization Task has been updated to re-encrypt all application attributes that are listed in the application's attribute named encrypted, and all out-of-the-box applications have been updated to correctly define their attributes with sensitive data.
(ETN:21425) Open and closed access request details are now shown in ServiceNow for access requests initiated in ServiceNow.
(ETN:21430) The advanced filtering on the entitlements tab of the View Identity page will now properly filter on account display name when data is entered.
(ETN:21432) Boolean operators in complex filter strings defined in Advanced Analytics identity searches are now correctly converted between advanced and basic searches.
(ETN:21434) Batched AccountRequests maintain the proper casing for request account attribute names.
(ETN:21441) Quicklink authorization is now correct when SSO is enabled.
(ETN:21443) The Workgroup Administrator capability now allows workgroup membership editing.
(ETN:21444) Multiple policy violations for an identity from the same policy constraint can now be mitigated correctly.
(ETN:21450) Identity Refresh will now correctly adjust role assignments when an assigned role is renamed.
(ETN:21459) Objects of type Custom will now have the correct object updated when re-imported.
(ETN:21461) Scrolling in the rule editor now works correctly in Internet Explorer 8.
(ETN:21465) The filename for CSV and PDF report exports will now be based on the report name.
(ETN:21466) The Account Attributes Live Report no longer includes duplicate information for accounts when multiple accounts with the same display name exist for an identity.
(ETN:21467) Delegated policy violations can now be revoked.
(ETN:21470) A role can now be cloned multiple times in the same login session.
(ETN:21471) Custom identity attributes displayed in Advanced Analytics identity search results are now included in a PDF export of the results.
(ETN:21473) Target aggregation tasks now correctly display the list of applications to select for aggregation.
(ETN:21475) The standalone REST authentication resource /rest/authentication now correctly authenticates users.
(ETN:21481) Advanced Search filters for an Identity Search in Advanced Analytics will now correctly filter an attribute of type Identity such as manager with a not equals operator.
(ETN:21491) Editing an account in the View Identity page for an account on an application where the identity has multiple accounts will now apply the edits to the correct account.
(ETN:21503) Email notification for rejection of role through its parent approval work item will now show the correct rejecter.

(ETN:21513) Performance of aggregating logical applications whose tiers were not explicitly included in the task has been improved.
(ETN:21514) Display names are now used for items in the target field when exporting results from Advanced Analytics Audit searches.
(ETN:21519) Remediation of required roles originally provisioned using assignment will now be done on the correct account in cases where a user has multiple accounts on the same application.
(ETN:21524) The match mode (any or all) of a multi-valued filter in report configurations are now persisted and viewed correctly.
(ETN:21525) SSO systems that use the Authorization HTTP header for a use other than BasicAuth are now supported.
(ETN:21529) Workflow launch messages of type lNFO are now displayed on the dashboard when a workflow is launched from a QuickLink.
(ETN:21532) The ServiceNow connector now has session pooling to improve performance and reduce the number of open sessions with ServiceNow.
(ETN:21534) Provisioning to multiplexed applications that do not support provisioning will now create manual work items instead of failing.
(ETN:21550) Submitting an access request for a role when using lnternet Explorer without specifying a sunrise or sunset date when sunrise and sunset dates are enabled will no longer fail.
(ETN:21553) LDAP-based connectors can now read group memberships for an account during account aggregation when the account has commas, parentheses, or asterisks in the cn portion of the account dn.
(ETN:21554) Long column header labels are now correctly displayed in the CSV export of reports regardless of the number of columns selected for inclusion in the report.
(ETN:21558) The certification access review detail grid will now contain wrapped complete text instead of text truncated to fit in the column.
(ETN:21562) Rules can now be edited in the attribute editing page of the ldentity Mappings configuration.
(ETN:21563) Adjustments to column sizes for approval work item grids will now be saved and used on subsequent views of work items.
(ETN:21565) The Oracle Database - Direct connector can now set user passwords that contain regex special characters.
(ETN:21567) The Manage Access Requests page now allows the logged in user to be used as a filter for the requester or requestee.
(ETN:21568) The tags filter in Advanced Analytics Access Review search will now be correctly displayed when refining a search.
(ETN:21574) Login will no longer fail when the browser timezone contains multiple daylight savings time periods or the browser timezone is not represented in the application server JDK timezone database.
(ETN:21581) The Lotus Domino connector will now honor the multi-valued configuration of schema attributes by returning attributes as a list even if the attribute is a single value.
(ETN:21582) Scoping rules are now applied to accessibility of Access Reviews for users with the Certification Administrator capability.
(ETN:21587) Scopes associated with Task Definitions will now cascade to Task Schedules as well as Task Definitions.

(ETN:21590) Workflow tracing can now be globally enabled using log4j by configuring trace level logging on the sailpoint.WorkflowTrace class.
(ETN:21591) SAML authentication is now supported for an Identity Provider that uses HTTP query parameters.
(ETN:21595) Completed certifications can no longer be forwarded.
(ETN:21597) Dashboard Policy Violation quick link count now reflects both policy violations owned by current user and owned by workgroup that current user is a part of.
(ETN:21600) Entitlement tooltip descriptions are now displayed for entitlements that are shown in the remediation dialog of a certification.
(ETN:21605) Login will no longer fail when using a browser that does not provide a value in the User-Agent HTTP header.
(ETN:21620) The Oracle Database Direct connector will no longer fail when creating and modifying accounts due to attempts to assign a QUOTA to the DEFAULT_TABLESPACE.
(ETN:21625) The Active Directory connector now terminates an aggregation if it receives a PartialResultException from Active Directory. To allow the aggregation to continue ignoring the ParitalResultException, set the application attribute allowPartialResultException to true.
(ETN:21642) Messages from the Perform Maintenance task related to re-assigning work items from disabled users will now be localized using the application server's locale.
(ETN:21643) The LDAP connector now uses the account aggregation task's **Enable partitioning** option rather than the presence of partition definitions in the application to control whether partitioned aggregation is used.
(ETN:21650) Mainframe connectors will now aggregate permissions for groups that do not have members in the native security system.
(ETN:21666) Custom forms associated with work items where approval decisions are required will now have proper dynamic processing enabled when postback fields are updated.
(ETN:21683) The Host Configuration page is now properly localized.
(ETN:21687) The Page label in the bottom toolbar for tables is now correctly displayed in the Spanish locale.
(ETN:21693) The Identity Request for a Forgot Password request is now correctly set to ForgotPassword.
(ETN:21704) The active and archive work item tables on the Manage Work Items page will no longer truncate columns when other columns are resized to large widths.
(ETN:21727) Keep alive messages sent to mainframe agents are now encoded in the proper character set to prevent parsing errors when received.
(ETN:21728) The **Add to Cart** button in Lifecycle Manager requests can no longer be pressed multiple times.
(ETN:21729) Certification lifecycle dates displayed when editing active certifications are now more accurate.
(ETN:21746) Pooling for rule and script execution has been improved to be more resilient.
(ETN:21753) **SECURITY:** The activeTab parameter of the Manage Work Items page is no longer vulnerable to Cross-site Scripting.
(ETN:21754) **SECURITY:** Persisting Manage Work Items table state (column size and sort order) is no longer vulnerable to Cross-site Scripting.

(ETN:21764) When merging accounts using Manual Correlation takes longer than 60 seconds, an informational message is now presented to the user.
(ETN:21765) A warning is no longer displayed when submitting Lifecycle Manager requests and an approval is assigned to a workgroup without an email address and the workgroup is configured to not receive notifications.
(ETN:21775) ServiceNow session management is now improved for long running aggregations to enable recovery from invalidated sessions.
(ETN:21790) An exponential backoff algorithm has been implemented in the Google Apps connector to handle server throttling restrictions in the Google Apps environment.
(ETN:21793) iiq-custom.css has been updated to include more examples and documentation to aid in branding.
(ETN:21796) Partition names for the JDBC connector based on the partition SQL statement will now be truncated as appropriate. Alternatively, the partitionNames application attribute can be used to define custom partition names.
(ETN:21797) When a partitioned aggregation fails to start, the task is marked with a failure.
(ETN:21799) Authentication for electronic signatures will now work correctly when used in generic work items.
(ETN:21824) Buttons in modal dialogs will now display in the appropriate language when the browser language is changed without restarting the browser.
(ETN:21829) The Active Directory connector can now support the root domain configured as the search DN.
(ETN:21862) When a role is approved by a member of the workgroup that owns it the audit event source will now be set to the approver identity rather than the workgroup.
(ETN:21868) **Minimum Character Type** will now be properly enforced across multiple password policies during password requests in Lifecycle Manager when **Synchronize Passwords** is selected.
(ETN:21873) Connection management between IdentityIQ and the Connector Gateway has been made more resilient.
(ETN:21874) Stored procedures to install in Oracle E-Business are now provided to allow connector operations to have the required access to native stored procedures.
(ETN:21880) Role composition access certifications now properly display HTML embedded in profile descriptions.
(ETN:21885) The Forwarding User identity select in the Attributes tab of the View Identity page will now remain visible after transitioning to another tab and back to the Attributes tab.
(ETN:21889) The Microsoft Forefront Identity Manager (FIM) Provisioning Integration Module (PIM) now supports FIM setup with the FIM Web Service and FIM Sync Service running on different hosts.
(ETN:21901) Checking the status of a queued provisioning request sent through an implementation of the IntegrationExecutor interface should now use the checkStatus method instead of the getStatus method.
(ETN:21926) If using full text index search for LCM Request Access, will need to re-run the Full Text Index Refresh task to generate new combined index for searching.
(ETN:21930) The identity model can now support link/account attributes with @ in the name.
(ETN:21956) The example rule Example Ticket Plan Generation Rule has been updated to demonstrate how the rule must scan the Identity Request in order to accurately update the SRM ticket with a Closed status.

(ETN:21969) When completing a remediation item the currently logged in user is now made the owner of the remediation item.
(ETN:22015) Multiple duplicate ProvisioningRequests associated with integration configs will now be properly assimilated rather than duplicated.
(ETN:22018) Exporting objects from the console with -clean will no longer filter strings that are not XML elements.
(ETN:22034) Role descriptions indexed in the Lifecycle Manager full text index are now stored in UTF-8 to allow for accurate search results.
(ETN:22042) The PeopleSoft and PeopleSoft HRMS connectors now support the use of a domain connection password.
(ETN:22049) Login will no longer fail when using a browser that does not provide a value in the User-Agent HTTP header.
(ETN:22061) The Oracle E-Business connector now supports the EMPLOYEE_ID attribute.
(ETN:22063) Role access requests with a sunset date between the request date and approval date are no longer provisioned to the identity.
(ETN:22070) Required and permitted roles are now correctly detected when **No automatic detection with profiles unless assigned** is enabled.
(ETN:22074) Entitlement Owner Access Reviews now consistently use the entitlement display name when showing the entitlement information.
(ETN:22103) Aggregation from CyberArk will now aggregate accounts that do not have any associated permissions.
(ETN:22104) Certifications containing revocations of deleted users will no longer report opened actions - the actions will now be correctly marked completed.
(ETN:22125) Role statistics will now include modify requests as well as create requests.
(ETN:22142) The Active Directory connector has been enhanced to include more specific information during failure conditions.
(ETN:22143) Failure during delta aggregation processing will now more accurately save the current state to prevent duplicate processing when resuming the aggregation.
(ETN:22145) The reminder link in access review work items that have been completed are now disabled.
(ETN:22168) All entitlement descriptions in approval work items are now displayed when you hover over the icon.
(ETN:22185) Certification escalations and related email notifications will now happen if appropriate on the on the certification expiration day.
(ETN:22193) Performance of the filters for the Inbox and Outbox have been improved.
(ETN:22207) **SECURITY:** The Apache HTTP client library has been updated to mitigate a published vulnerability related to man in the middle attacks.
(ETN:22223) The Active Directory connector will now honor domain-specific host settings and will no longer fallback to the generic host attribute.
(ETN:22257) The requestee of a Lifecycle Manager access request can now cancel the request from the Manage Access Requests page.

(ETN:22259) The certification email template is now provided the certification owner name using the ownerName variable.
(ETN:22268) Account Group aggregation now correctly adjusts account group hierarchy to reflect the managed system state.
(ETN:22269) The Active Directory connector will now correctly aggregate group membership changes for a group with more than 5000 members when delta aggregation is used for an application that is configured for multiple Active Directory domains.
(ETN:22270) SAML based SSO is now compatible with ADFS.
(ETN:22275) lf a member of a workgroup click on the quicklink from dashboard for approval workitems, the items owned by the workgroup are now loaded correctly.
(ETN:22316) The display name of the role is now displayed in the Allowed By column in the Identity Entitlements tab. lf the role does not have a display name then the role name is shown.
(ETN:22331) An entitlement profile with an entitlement value containing underscore can now be edited in the role modeler.
(ETN:22433) Forgot Password will now work when an Active Directory application is used as the pass through authentication application and the Active Directory application is configured with a searchDNs configuration with multiple entries with the same searchDN value.
(ETN:22437) Exporting role mining results to CSV will now work without an error.
(ETN:22448) The maximum length of a localized attribute description when importing from CSV is now 1024 characters.
(ETN:22462) Performance has improved for account aggregation using the Google Apps connector.
(ETN:22464) The Oracle Database connector now supports creating an external user.
(ETN:22466) Display of localized attributes will now fallback through the locale hierarchy showing the first available attribute value from variant to country to language locale to default locale.
(ETN:22476) The CLI console now contains an echo command.
(ETN:22480) Rules run as Rule Executor tasks can now query the TaskResult object to determine if termination of the task has been requested to take appropriate action to halt. The new method for TaskResult is public boolean isTerminateRequested().
(ETN:22492) **SECURİTY:** The restricted browser used in Desktop Password Reset has been hardened to prevent unauthorized system access using combinations of drag-n-drop and button presses from keyboard buttons that emulate mouse clicks.
(ETN:22498) The certification signer shown in the My Access Reviews table views now shows the signer's display name.
(ETN:22553) Provisioning plans with attribute requests' value set to null will now be allowed to be marked completed by the identity request and remediation scanner.
(ETN:22578) The entitlement values in the access review filter definition are now sorted.
(ETN:22585) Account attributes are now promoted correctly following an account revocation.
(ETN:22586) Error handling has been improved in partitioned tasks.
(ETN:22607) The value of the **Number of minutes a user will be locked out due to unsuccessful login** setting now displays properly for values larger than 32,000.

(ETN:22631) **SECURITY:** SQL Injection vulnerabilities related to account names in the DB2 Connector have been remediated.
(ETN:22646) Administrative reset of Lotus Domino HTTP passwords greater than 14 characters no longer fails.
(ETN:22648) Disabled the ability to forward a completed certification from the Access Review Completion Status page.
(ETN:22659) SNC Configuration parameters for SAP applications can now be defined and edited in the application web user interface.
(ETN:22662) Accounts or groups in the SAP Portal application can now be previewed in the application edit user interface more than once.
(ETN:22698) Sorting of items in the remediation items list in a remediation work item is now consistent when items for the same identity crossed table paging boundaries.
(ETN:22700) The Lotus Domino connector now correctly processes attribute value change requests and no longer creates a group with the name of the attribute value.
(ETN:22725) The Lotus Domino connector can now rename a user at the same time it is enabled or disabled.
(ETN:22736) The OAuth Bearer Token field for the SCIM connector is now displayed as a password field in the application edit user interface.
(ETN:22746) The **Edit My Preferences** link will now work when used on the View Identity page.
(ETN:22771) Connector error messages during password reset operations are no longer displayed twice in the task result.
(ETN:22805) Custom forms in Lifecycle Manager work items will now be properly initialized so that input data will be correctly displayed.
(ETN:22810) The SQL Server connector will now delete both the server login and the database user login when processing account delete requests.
(ETN:22814) Approval statuses in identity requests will now be properly maintained during the entire Lifecycle Manager workflow.
(ETN:22816) The popup calendar available for date fields will now display localized strings correctly.
(ETN:22826) Incorrect use of equality operators identified by static code analysis have been fixed.
(ETN:22873) The Google Apps connector will now correctly process changes to multi-valued attributes when the value to be set is a list.
(ETN:22876) The Account Group Membership Access Review Live Report, Account Group Permission Access Review Live Report, and Entitlement Owner Access Review Live Report will no longer fail when using Oracle as the application database.
(ETN:22899) Exporting Advanced Analytics Access Requests search results to PDF will now succeed when Verified Date is included in the displayed columns.
(ETN:22910) The dialog to select a remediator to provision missing roles in an access review will now display correctly.
(ETN:22926) Notification time lines displayed when viewing certification properties are now correctly displayed for a certification that was initially staged and then activated.

(ETN:22931) Changing the HTTP Password for Lotus Domino can now be achieved without the current password. If the ID file password is also to be changed, an account attribute named IDFileCurrentPassword must be included in the password change provisioning plan.
(ETN:22933) The UNIX password interceptor client can now be installed in a directory other than `/etc/PWI`.
(ETN:22945) The certification phase transition processing in the Perform Maintenance task has been improved to not keep a database cursor open during the entire processing time.
(ETN:22950) The tool tip for the History list in a Lifecycle Manager approval now shows the correct help text.
(ETN:22955) The width attribute of a field will now be honored when a form is rendered.
(ETN:22959) Performance of certification generation using partitions has been improved.
(ETN:22968) The Value field for account type attributes in the Advanced Search section of Advanced Analytics Identity searches is now always visible.
(ETN:22969) Accounts created during an aggregation will no longer be marked for deletion when the **Detect Deleted Accounts** aggregation task argument is enabled.
(ETN:22974) The end_date attribute will no longer default to 01/01/2222 when creating or modifying an Oracle Applications user.
(ETN:22981) The web service stubs for managing Salesforce have been updated to version 32.0.
(ETN:22990) SMTP password and confirm password are now kept synchronized if there are errors when saving the configuration.
(ETN:23011) The certificationItem and workItem objects are now available to template processing for certification challenge email templates.
(ETN:23015) The Active Directory connector will no longer fallback to the generic connection host when domain-specific connection hosts are defined.
(ETN:23016) Account and account group aggregation performance has been improved for the Salesforce connector.
(ETN:23068) The text "cer" will no longer be incorrectly localized into an empty string when displayed in the user interface and reports.
(ETN:23073) Empty access reviews in a staged certification with automatic signoff enabled will not be signed off until the certification is activated.
(ETN:23099) Partitioned aggregation for LDAP-based connectors will now use the appropriate searchDN values in each partition.
(ETN:23110) Role details dialogs across the product will now display profiles using the simplified entitlement view when basic profiles are defined.
(ETN:23134) A delegated work item created by a delegation rule for a certification created by a certification event will now be correctly created.
(ETN:23153) The table layout options for sorting and column selection are now correctly localized.
(ETN:23161) Top-level workflows can now be selected as a subprocess in the Business Process Editor.
(ETN:23162) The Active Directory connector will now treat provisioning requests without an explicit operation as a modify request.

(ETN:23165) Using the back button during identity editing to select a different user will no longer result in presenting the previous user's data.
(ETN:23204) Provisioning using the Siebel connector now work when using a non-administrative user to access Siebel.
(ETN:23212) Invalid SSL certificates when **SSL Server Certificate Validation Required** is disabled in Desktop Password Reset will now be detected in non-English locales.
(ETN:23253) Logical application entitlements will no longer be duplicated when the **Refresh Composite Applications** option is enabled during an Identity refresh.
(ETN:23262) The Manual Correlation user interface now supports multiple account attribute check boxes for inline account status editing.
(ETN:23272) Sunset dates for Lifecycle Manager entitlement access request are now properly processed when due.
(ETN:23308) Identity attributes promoted with a non-String type will retain any later manual changes until the feed value changes when edit mode is set to Temporary.
(ETN:23329) The SAP Portal connector now supports setting the productive password to prevent the user from having to change the native password again on first use.
(ETN:23372) Multiplex applications managed by an IntegrationConfig will no longer result in provisioning errors during fulfillment of Lifecycle Manager access requests nor require the PROVISIONING feature string to function.
(ETN:23400) The form type selection when creating a new form in the Form Editor will no longer be hidden when creating multiple forms before leaving the Form Editor page.
(ETN:23406) The Workday connector now supports aggregating accounts without a user id.
(ETN:23408) The identity list web service used by many tables now has protections against invalid sort requests caused by mis-configured table view or customizations.
(ETN:23427) The SunOne LDAP connector can now consistently process changelogs in delta aggregation by using the nsUniqueId attribute as an identifier. This requires a configuration change on the LDAP server documented in the *Direct Connectors Administration and Conjiguration Guide*.
(ETN:23447) The simplified profile entitlement display is now shown in the role details section of Lifecycle Manager access request approval work items.
(ETN:23473) RoleDetections corresponding to roles that are both assigned and detected now properly reference their corresponding role assignment.
(ETN:23511) The **Return to dashboard on timeout** configuration will now be honored when SSO is enabled.
(ETN:23523) Signed re-assigned certifications can no longer be returned or modified.
(ETN:23617) Enabling trace level logging on sailpoint.web.SailPointNavigationHandler (directly or indirectly) will no longer cause a stack overflow.
(ETN:23635) When full text searching is enabled in Lifecycle Manager, contains searches are no longer supported.
(ETN:23642) The AIX connector no longer adds an extra trailing space to the gecos field during aggregation.
(ETN:23645) The SAP connector will now correctly read the User Last Logon Date attribute in non-CUA environments.

(ETN:23655) A new system configuration attribute named spNameQualifier is available that, when set, will override the entityId of the SAML config object as the SPNameQualifier entry of the request when using SAML-based SSO.
(ETN:23673) The Lotus Domino connector now correctly processes attribute value change requests and no longer creates a group with the name of the attribute value.
(ETN:23689) **SECURITY:** Knowledge of the internal database id of a work item will no longer allow access by an authenticated user to a read-only view of the work item.
(ETN:23716) The Perform Maintenance task will now lock work items during processing to ensure work items will only be processed by one task when concurrent tasks are running.
(ETN:23807) Test Connection for the ServiceNow connector will now work correctly before saving the application.
(ETN:23837) Date fields in forms will now display correct localized date formats.
(ETN:23877) Errors launching the workflow to process Lifecycle Manager password requests are now localized.
(ETN:23923) Revoking a role that is both assigned and detected no longer brings up an additional dialog asking to revoke it as a permitted role as well, because that action is already implied.
(ETN:23925) The Linux connector will now read the last login date for an account during aggregation.
(ETN:23943) The Active Directory connector will now use the same server for all operations related to creating and updating an account to prevent issues caused by replication delays.
(ETN:23947) The Active Directory connector will now allow using userPrincipalName as an authentication attribute for pass through authentication.
(ETN:23960) Provisioning using the Salesforce connector will now allow using Id as the account identity attribute.
(ETN:23963) Revoking a role which is both assigned and detected now removes the roles entitlements from the identity.
(ETN:24069) The Salesforce connector now supports email addresses that contain an apostrophe.
(ETN:24073) Request objects to run scheduled assignment workflow at sunset date will now be created when using manual provisioning, a sunset date, and no sunrise date.
(ETN:24090) The requester in a Lifecycle Manager access request is now allowed to add comments to a work item for the request.
(ETN:24251) Forgot Password will now use the authentication attributes defined on the pass through application in addition to the display name and identity name when finding an identity match.
(ETN:24366) The Apache commons-logging and log4j libraries included in the product have been updated.
(ETN:24395) The restricted browser used in Desktop Password Reset will now close after confirmation from the user that they wish to close the browser.
(ETN:24404) Connector Gateway supports JDK 1.8
(ETN:24429) The activation date for a role assignment can now be changed from the View Identity page without a JavaScript error.
(ETN:24519) The LDAP connector no longer has LDAP server connection leaks related to fetching group membership for an account during account aggregation.

(ETN:24527) The Cloud Gateway is now more resilient to processing errors and warnings returned from the connector.

Known Issues

(ETN:19009)
Problem: In some deployment scenarios, the path to the SIGAR library cannot be determined and a message such as "Sigar library for CPU stats is not on the library path: <path>" or "Unable to use Sigar: UnsatisfiedLinkError" is shown in the application server logs.

Workaround: Add the fully qualified directory path of the deployed `WEB-INF/lib` directory to the `java.library.path` list.

(ETN: 21358)
Problem:
The iiq exportschema and iiq exportviews commands can intermittently fail with a "java.lang.IllegalStateException: Pool not open" error.

Workaround:
Re-run the command.