SailPoint IdentityIQ

Version 8.1

User Guide

Table of Contents

IdentityIQ Introduction

SailPoint IdentityIQ is an identity and access management solution for enterprise customers that delivers a wide variety of IAM processes-including automated access certifications, policy management, access request and provisioning, password management, and identity intelligence. Furthermore, IdentityIQ has a flexible connectivity model that simplifies the management of applications running in the datacenter or the cloud.

Compliance Manager — IdentityIQ Compliance Manager automates access certifications, policy management, and audit reporting through a unified governance framework. This enables you to streamline compliance processes and improve the effectiveness of identity governance, all while lowering costs.

Lifecycle Manager — IdentityIQ Lifecycle Manager manages changes to access through user-friendly self-service request and password management interfaces and automated lifecycle events. It provides a flexible, scalable provisioning solution for addressing the constantly evolving access needs of your business in a way that's both efficient and compliant.

IdentityAI – Integrating IdentityAI within IdentityIQ enables the delivery of Predictive Identity. IdentityAI is a rule based machine learning engine using identity graph technology to provide recommendations for access review and access request decisions. With IdentityAI enabled, you can also review access history for identity cubes, create dashboards that can be customized from an administrative perspective, and view peer groups within the IdentityAI user interface.

Privileged Account Management Module — IdentityIQ Privileged Account Management module provides a standardized approach for extending critical identity governance processes and controls to highly privileged accounts, enabling IdentityIQ to be used as a central platform to govern standard and privileged accounts.

Connectors and Integration Modules — IdentityIQ offers Integration Modules that support the extended enterprise IT infrastructure. Third party provisioning and service desk integration enable multiple sources of fulfillment to access change. Service catalog integration supports a unified service request experience with integrated governance and fulfillment. Mobile device management integration mitigates risk posed by mobile devices through centralized visibility, control and automation. And IdentityIQ's IT security integration provides enhanced security with improved responsiveness and controls.

Open Identity Platform — SailPoint's Open Identity Platform lays the foundation for effective and scalable IAM within the enterprise. It establishes a common framework that centralizes identity data, captures business policy, models roles, and takes a risk-based, proactive approach to managing users and resources. The Open Identity Platform is fully extensible, providing robust analytics which transforms disparate and technical identity data into relevant business information, resource connectivity that allows organizations to directly connect IdentityIQ to applications running in the datacenter or in the cloud, and APIs and a plugin framework to allow customers and partners to extend IdentityIQ to meet a wide array of needs. An open platform allows organizations to build a single preventive and detective control model that supports all identity business processes, across all applications-in the datacenter and the cloud. SailPoint IdentityIQ applies consistent governance across compliance, provisioning and access management processes, maximizing investment and eliminating the need to buy and integrate multiple products.

Password Manager — IdentityIQ Password Manager delivers a simple-to-use solution for managing user passwords across cloud and on-premises applications policies from any desktop browser or mobile device. By providing intuitive self-service and delegated administration options to manage passwords while enforcing enterprise-grade password, IdentityIQ enables businesses to reduce operational costs and boost productivity.

Amazon Web Services (AWS) Governance Module — Enables organizations to extend existing identity lifecycle and compliance management capabilities within IdentityIQ to mission-critical AWS IaaS environments to provide a central point of visibility, administration, and governance across the entire enterprise. This includes policy

discovery and access history across all organization accounts, provisioning AWS entities and objects, access review and certification, and federated access support.

SAP Governance Module — Improves the user experience by introducing a new integrated visual interface for navigating and selecting SAP identities and roles as part of IdentityIQ lifecycle management and compliance solution. SAP data is presented in a familiar hierarchy format that closely represents deployed system resources and organizational structures. New filtering capabilities enable more efficient browsing and selection of SAP data so tasks can be performed faster. Improved granular support for separation of duty (SOD) violation policies provides flexibility for customers to craft more detailed identity governance policies that include SAP role details such as T-Codes and Authorization Objects.

Section I Certification

This section contains information on the following:

- "Certification Overview" on page 5 — description of the certification process.
- "Access Review Pages" on page 15 — view the access reviews assigned to you.
- "Targeted Certifications" on page 21 — overview of targeted access reviews.
- "Manager, Application Owner, Advance Certifications" on page 25 — overview of identity access reviews.
- "Role Membership and Entitlement Owner Access Reviews" on page 29 — overview of object access reviews.
- "Role Composition Access Reviews" on page 33 — overview of role composition access reviews.
- "Account Group Membership and Account Group Permission Access Reviews" on page 37 — overview of account membership and account group access reviews.
- "Access Review Decisions/Operations" on page 41 — overview of the access review decisions and operations available.
- "How to Complete Access Review Work Items" on page 47 — overview of work items associated with access reviews.
- "Certification Events" on page 51 — define certification events.
- "Manage and Schedule Certifications" on page 59—create and schedule certifications and access reviews from the Certifications page.

Chapter 1: About Certifications

In IdentityIQ, certifications let you automate the review and approval of identity access privileges. In a certification, IdentityIQ collects fine-grained access or entitlement data, and formats the information into interactive reports, which are sent to the appropriate reviewers as access reviews. You can also use certifications to validate things like roles (verifying that they contain the right privileges) and account groups (making sure the right people are in it).

Certifications typically consist of multiple access reviews. For example, when you schedule a Manager Certification (a type of certification that asks managers to review and validate their direct reports' access), it will consist of an individual access review for each of the managers you opt to include as part of the campaign. However, it is possible to configure a certification such that it includes only one access review - for example, you might schedule a Manager Certification for just one specific manager, which means that there would only be one access review making up that certification.

When you configure the certification, you can set it up to annotate each access review with descriptive language that highlights changes, flags anomalies, and highlights where policy violations appear. The access reviews enable reviewers to:

- Approve access for identities
- Approve account group permissions and membership
- Approve role composition and membership
- Take corrective actions, such as revoking entitlements that violate policy
- Forward, reassign, or delegate all or part of the access review to another reviewer

For all corrective actions, IdentityIQ can fulfill certification revocations through automated or manual means, depending on the individual applications' connector configurations. IdentityIQ can also be configured to integrate with ticketing systems or other provisioning systems to fulfill provisioning requests.

The sections below will familiarize you with some terms and concepts related to certifications.

Certification Schedules

Certifications can be scheduled to run on a **periodic** basis; they can also be triggered by an **event**, or run as a **one-off** process.

Periodic Certifications

Periodic certifications are scheduled to run on a recurring basis, such as daily, weekly, monthly, quarterly, or annually. These periodic access reviews provide a snapshot view of the identities, roles, and account groups within your enterprise. Periodic certifications focus on the frequency at which entire entities (identities, roles, or account groups) must be certified.

A periodic certification is considered complete when *all* the access reviews contained within the certification have been completed. The access reviews that make up the certification, in turn, are considered complete when all items, such as roles, entitlements, violations, and application objects, have been acted upon, and those decisions are confirmed by the user to whom that access review was assigned.

Periodic certifications can be created using a multi-level sign-off structure, to allow multiple certifiers to review the access before the review is considered complete.

Event-Based Certifications

Certifications can be configured to run based on "trigger" events that occur within IdentityIQ. For example, you can configure IdentityIQ to automatically generate a certification any time an identity's manager changes. You can also configure the events that trigger the certifications to meet the needs of your enterprise.

One-Off Certifications for Identities

One-off certifications can be created from the Identity Risk Score, Identity Search Results, or Policy Violation pages. These one-off access reviews can be run for a single identity, or for multiple identities at once. One-off certifications are most often used in special situations, such as when an access review is required outside of the normal certification cycle. You can also schedule standard IdentityIQ certifications to run on a one-off basis.

Types of Certification

IdentityIQ provides these types of certification:

- **Targeted Certifications** — the most flexible type of certification, designed to meet most organizations' full range of certification needs from a single place. In a Targeted Certification you can certify role, entitlement, and account access for a narrowly defined set of your users. The Targeted Certification gives you a high level of flexibility in choosing which parameters to include in the certification (such as who, what, and when to certify).

- **Manager Certifications** — certify that a manager's direct reports have the right entitlements they need to do their job, and no more than that. You can configure a Manager Certification to include all managers in the company, or only specific managers. You can also configure which applications you want to certify as part of the Manager Certification.

- **Application Owner Certifications** — certify that all identities that have access to *applications* for which the reviewer is responsible have the proper entitlements.

- **Entitlement Owner Certifications** — certify that all identities that have access to *entitlements* for which the reviewer is responsible are correct.

- **Advanced Certifications** — certify entitlements and roles for all identities included in a specific population or group.

- **Account Group Membership Certifications** — certify that all accounts which make up an account group are correct - that is, are the right accounts in the account group. Account groups that do not have owners assigned are certified by the owner of the application on which they reside.

- **Account Group Permissions Certifications** — certify that all permissions that are granted to an account group for selected application(s) are correct. Account groups that do not have owners assigned are certified by the owner of the application on which they reside.

- **Role Membership Certifications** — certify that roles for which the reviewer is responsible are assigned to the correct identities.

- **Role Composition Certifications** — certify that roles for which the reviewer is responsible are composed of the proper permissions and entitlements.

- **Identity Certifications** — this type of certification is used for "one-off" certifications that are launched from the Identity Risk Score, Identity Search Results, or Policy Violation pages. These certifications verify the entitlement information for the identities, typically for at-risk users.

- **Event-Based Certifications** — certify the entitlement information for the identities selected based on events detected within IdentityIQ.

Contents of a Certification: Policies, Roles, and Entitlements

These are some common terms that are used in certifications.

- **Policies** that govern access can be defined for your enterprise, and you can use certifications to monitor users that are in violation of those policies. For example, a separation-of-duties policy may dictate that one person can not both request and approve purchase orders, or an activity policy might dictate that a user with the Human Resource role should not be able to update the payroll application.

  In access reviews, Policy Violations show any violations of policy for an identity. The access reviewer(s) must take action on these violations before the certification can be completed.

  There is a Policy Violations page in IdentityIQ that is separate from the access review page. Policy violations can be viewed and acted upon from this page, or as part of another access review.

  > **Note:** **Decisions made on a violation that come from another page or review are displayed within the access review, below the summary information, or in the revocation dialog.**

- **Roles** are essentially collections of permissions. Through roles, system entitlements can be grouped together and presented as a logical unit, such as a job function, rather than as a detailed and often difficult-to-interpret list of access rights. Within IdentityIQ, users are granted permissions through the roles that are assigned to them, or through roles they inherit through a role hierarchy.

  In an access review, only the top-level roles are displayed in the roles section. For example, if a role contains required and permitted roles, only the top-level role is displayed and the required and permitted roles are certified as part of that role. You can click on **Details** (in the three-line menu for the item) to expand the role information and view the role details and hierarchy. Both assigned and detected roles are displayed in the roles section.

  If an identity has a role assigned to it multiple times - for example, to grant the same access to multiple accounts the user holds - that role is displayed multiple times, and each one must be reviewed and acted on individually.

- **Entitlements** are either permissions, or specific values for an account attribute (such as group membership). In the context of certifications, entitlements refer to all the entitlements an identity has access to that are not included as part of a role that is assigned to the identity.

  Certifications can also include IdentityIQ capabilities and scopes; if the certification includes capabilities and scopes, these appear as additional entitlements on the IdentityIQ application, as Capabilities and Authorized Scopes attributes. Revoking these entitlements has auto-remediation enabled by default. This means that when the revocation is processed (either when the access review is signed, or immediately, based on the certification configuration) the capabilities and authorized scopes are removed from the identity.

For addition information see "Access Review Page Overview" on page 15.

Challenges

When an access reviewer has determined that the user's access should be revoked, you may want to allow the affected user to challenge the decision - for example to share information with the reviewer about why they may need to retain the access in question. To allow users to challenge revocation decisions, you enable a **challenge period** as part of a certification's configuration. During the challenge period, if the certifier has revoked (for example) a user's Financial Reporting access, that user would get an email saying that the entitlement has been revoked; the user can then respond with comments on the item describing why they need to keep access to the

Financial Reporting system. The certifier sees that the revocation has been challenged and why, and is able go back in to the access review and reconsider their decision.

For more information, see "How to Challenge a Revocation Request" on page 49.

Revocations

Revocation is when an identity's entitlements are altered in the source application, to remove any entitlements that were marked by the access reviewer as needing to be revoked. Depending on the provisioning features in use, remediations may be processed *manually* or *automatically*. If automatic provisioning is enabled in your system for the relevant application, revocation of access can happen without any further action from the reviewer, as a consequence of an access review decision. If the relevant application does not have automated provisioning enabled, then remediation of that application's entitlements is managed by the creation of manual work items for the Application Revoker or Application Owner, requesting that they change the identity's access or permissions manually. IdentityIQ alerts the Application Revoker or Application Owner about the manual work item via an email message.

A Revocation phase can be enabled for the certification as part of the certification setup. Note that remediation of access occurs as a result of revocations in an access review whether or not a Revocation period is enabled. The difference is that when a Revocation period is enabled, IdentityIQ *monitors* the status of remediation requests; when it is not enabled, remediation requests are submitted for processing but are not tracked.

Escalations and Reminders

When a person who has been assigned a manual work item for revoking access does not complete the work in a timely manner, IdentityIQ can send that person email reminders or can even escalate the work to the next level, such as to their manager. Revocation reminders and escalations are used only when revocation is being handled through manual work items assigned to the application's revoker or owner, and not when revocation is processed automatically.

The remediation parameters that are set in the certification configuration tell IdentityIQ what reminders and escalations to perform, and when.

Revocation reminder emails can be automatically sent to the person assigned the revocation work item if the work item is not completed within a specified timeframe. Reminders can configured to be sent once, or at scheduled intervals, beginning a specified number of days before the end of the Revocation period.

Escalations can also be automated to notify and transfer control to someone else (for example, the revoker's manager, or the application owner) if the person originally responsible for the revocation has not completed it, and the end of the Revocation period is near. Escalation triggers, email templates, and rules for determining who the item is escalated to are all part of the Certification configuration.

Phases of a Certification

Certifications progress through phases as they move through their lifecycle. The phases associated with each certification are determined when the certification is set up. Some phases are part of every certification, while others are optional phases that can be configured as needed according to your organization's business processes.

- **Staging** — this is an optional phase you can use to test or validate a certification before sending it to reviewers. The staging phase lets you create a certification and associated access reviews, but not send the access reviews to the certifiers. You can view what the certification schedule definition produces before the certification is activated. If the generated certification does not match your needs, you can cancel the certification and redefine it as needed. If the certification is accurate, you can activate it. If you want to use a staging period, you enable it as part of the certification's configuration parameters at the time you set up the certification.

- **Active** — the active phase is the review period when the reviews are performed - that is, when all decisions that are required for the access review are made. During this phase, reviewers make decisions about access, and changes can be made to these decisions as frequently as required, until the access period expires. The active period lasts either for a scheduled amount of time, or until all the access reviews for the certification have been signed off. You can sign off on the active stage if no roles or entitlements were revoked, or if the optional challenge period has not been enabled. When you sign off on a periodic certification it enters either an end phase, or, if enabled, a revocation phase. To enter the revocation phase, the revocation period must be enabled, and at least one revocation decision must exist.

- **Challenge** — the challenge phase is an optional period when users can challenge all revocation requests if any of their roles, entitlements, or account group access are being removed. When the challenge phase begins, a work item and email are sent to each user affected by a revocation decision. The notifications contain the details of the revocation request and any comments added by the reviewer. The affected user has the duration of the challenge period to accept the loss of access, or challenge that decision. If you want to allow a challenge period, you enable it as part of the certification's configuration parameters at the time you set up the certification.

  You can sign off on a certification in the challenge phase if all challenges are complete and no open decisions remain for the access review. When you sign off on an access review, it enters either the end phase, or, if

enabled, the revocation phase. To enter the revocation phase, the revocation period must be enabled, and at least one revocation decision must exist.

- **Revocation** — the revocation phase is the period when all revocation work is completed. When the revocation phase is entered, revocation can be done either automatically or manually. Automatic revocation can happen if your provisioning provider is configured for automatic revocation or if your implementation is configured to work with a help desk solution and a help ticket is generated. If you don't have an automatic revocation process enabled, revocation is done manually via work requests assigned to the relevant users in IdentityIQ. For periodic certifications, the revocation phase starts when a periodic certification is signed off, or when the active and challenge phases have ended.

  Revocation activity is monitored to ensure that inappropriate access to roles and entitlements is revoked in a timely manner. Revocation completion status is updated at an interval specified during the deployment of IdentityIQ. By default this is performed daily. You can view detailed revocation information by clicking the "information" icon in the access review then clicking the **Details** button on the information dialog. Revocation requests that are not acted upon during the revocation phase can be escalated as needed.

- **End** – If a Revocation phase is not enabled for the certification, revocations can be done during the end period. The end period also indicated when the access review is complete.

Automatic Closing of Certifications

Automatic Closing is an option you can enable in your certifications, to handle access reviews that have not been completed by the time the certification's designated active period has ended. With automatic closing, you can automatically make decisions on the open line items – either to revoke, allow, or mark as an exception – or you can run a rule to perform more complex analyses or other actions.

If you choose to enable Automatic Closing, there are several configuration options you will set, including the amount of time to allow after the expiration date before automatic closing is invoked, any closing rule that will be run at that time, which action to take on uncompleted Access Review items, and any comment to add to each item for which the automatic action is taken. These can be set as global defaults, and also can be set (or changed from the global defaults) at the individual certification level.

Rules in Certifications

Certifications can use rules to customize certification behavior. Rules allow you to insert your own logic to modify the behavior of the certification; for example, you could write a rule to exclude your executive management team from certifications, or to add an additional level of sign-off approval to an access review. Rules are written using BeanShell, a lightweight Java-based scripting language. IdentityIQ provides a standard set of example rules that you can import to use as starting points for developing your own rules, in an *examplerules.XML* file.

When you set up a certification, there are numerous places where you can choose rules to modify the certification's behavior. Every rule has a type that categorizes it, and in certifications, the rule type determines where and how in the certification the rule can be used, and what kind of effect or purpose it has. Rules that are applicable to certifications are listed here, in the order in which they would be run in a certification.

Table 1—Rules in Certifications

UI Field Name	Rule Type	How/When Triggered	Effect/Purpose
Exclusion Rule	CertificationExclusion	Run as a part of the certification generation process	Excludes entitlements from the certification based on the rule's logic
Pre-delegation Rule	CertificationPreDelegation	Run as a part of the certification generation process	Automatically delegates access reviews based on the rule's logic
Who Do You Want to Certify Rule (Targeted Certifications Only)	CertificationScheduleEntitySelector	Run as a part of the certification generation process	Select identities to certify in a Targeted certification.
Group Factory: Certifier	Certifier	Run as a part of the Advanced certification generation process for Group Factory certifications	Assigns certifier for each group's access review
Active Period Enter Rule	CertificationPhaseChange	Run at the start of the Active period; the Active period is the period during which certifiers can examine their access reviews and make access decisions	Open-ended; depends on rule logic
Certification Escalation Rule	WorkItemEscalationRule	If the access review has not yet been finished and signed-off by the certifier at the time specified by the Escalation Trigger in the certification definition, this rule is run at that time	Transfers ownership of the access review to a different identity (often the certifier's manager or the certification owner)
Challenge Period Enter Rule	CertificationPhaseChange	Run at the start of the Challenge period (if enabled), which follows immediately after the Active Period ends; If Process Revokes Immediately is selected, Challenge period begins for each entitlement at the moment it is revoked and this rule runs once for each revocation	Open-ended; depends on rule logic

Table 1—Rules in Certifications

UI Field Name	Rule Type	How/When Triggered	Effect/Purpose
Closing Rule	CertificationAutomatic Closing	Run according to the timeframe specified in the Automatic Closing configuration in the certification definition (after the end of the Active phase -- or Challenge phase if enabled)	Open-ended; depends on rule logic
Sign-off Approver Rule	CertificationSignOffApprover	Triggered by certifier sign-off on an access review	Transfers ownership of the access review to a next-level approver who needs to approve the certification decisions made by the certifier; this rule enables two-level (or multi-level) signoff on an access review Exception: When a challenge period is included, the sign-off approver can only override approval decisions; revocation decisions made by the original certifier and seen by the access holder in a challenge work item (whether they challenge the decision or not) will not be changeable in the sign-off approver's certification view.
Revocation Period Enter Rule	CertificationPhaseChange	Run at the start of the Revocation period; the Revocation period immediately follows the Active period (or the Challenge period if it is enabled)	Open-ended; depends on rule logic

Table 1—Rules in Certifications

UI Field Name	Rule Type	How/When Triggered	Effect/Purpose
Revocation Escalation Rule	WorkItemEscalationRule	If the revocation work item has not yet been completed by the assigned revoker at the time specified by the Revocation Escalation Trigger in the certification definition, this rule is run at that time	Transfers ownership of the revocation to a different identity (often the revoker's manager or the application owner)
End Period Enter Rule	CertificationPhaseChange	Run at the beginning of the End period, which starts after all other periods configured for the certification are complete	Open-ended; depends on rule logic

Self-Certification

Self-certification means a user is allowed to be the certifier for his or her own access. Self-certification is often considered a security risk because it allows a user to approve and permit his or her own access, whether or not it is appropriate to his or her job. By default, IdentityIQ does not allow self-certification, other than for System Administrators. However, some organizations have business reasons for allowing self-certification, so there are configuration options to permit it. These can be set at the global level, or at the individual certification level.

Globally, self-certification options are set in the **gear menu > Compliance Manager** page's **Behavior** section. Global settings set the default configuration values for individual certifications, but these defaults can be changed when you configure individual certifications.

At the individual certification level, self-certification options are set on the **Advanced** page of the Certification configuration options for most types of certification; for Targeted certifications this option is set in the **Choose Certifier** section, under **Advanced Options**.

When allowing self-certification, you can choose who is allowed to self-certify: **All certifiers**, **System and Certification Administrators**, or **System Administrators only**. Which users are considered System Administrators or Certification Administrators is determined by the IdentityIQ capabilities the user has. Capabilities can be assigned directly to users, and also to workgroups. The "System Administrator" capability defines who is considered a System Administrator. For Certification Administrators, any IdentityIQ capability that includes the "CertifyAllCertifications" SPRight (such as the out-of-the-box "Certification Administrator" capability) defines the user or workgroup as a Certification Administrator, for purposes of being allowed to self-certify.

You can not configure IdentityIQ to exclude *all* users from self-certification, since excluding even your System Administrators from self-certifying can potentially lead to certifications that are impossible to complete.

When you allow users to self-certify, you can also choose an identity or workgroup to be the **Self Certification Violation Owner**. For users that are not allowed to self-certify, this is the identity or workgroup that will receive any items that would require a self-certification - that is, when the reviewer and the user whose access is under review are the same person. If a Self Certification Violation Owner is not chosen, any items that require self-certification will be shown as read-only to the reviewer in the access review.

Chapter 2: Access Review Pages

The layout of the access review pages can be customized during the configuration of IdentityIQ. The organization of the pages can vary from the descriptions in this documentation, the function of the product should not be affected.

This section contains information on the following topics:

- My Access Reviews Page — the access reviews assigned to you. See "My Access Reviews Page" on page 18.
- Access Review Details — detailed access review information and take the required actions. See "Access Review Page Overview" on page 15.

Access Review Page Overview

Use this page to review access review requests. The information displayed on this page is dependent on the access review type and options selected at scheduling.

There are five access review types:

- Targeted — used for Targeted certifications
- Identity — used for Manager, Application Owner, and Advanced certifications
- Object — used for Entitlement Owner and Role Member certifications
- Role Composition — used for Role Composition certifications
- Account Group/Application Object — used for Account Group certifications

Only top-level roles are displayed as line items. For example, if a role contains required or permitted roles, those roles are certified as part of the top-level role in the same way that the entitlements that make up a role are certified with the role.

If an identity has a role assigned to it multiple times, that role is displayed multiple times and each one must be reviewed and acted on individually.

All of the access review detail pages include the following information, but it might display differently depending on the access review type:

- Access Review Information – Displays the administrative and statistical information for the access review.
- Filter – Enables you to filter the information displayed on the page.
- Access Review Decision Tab – Displays the list of items that must be certified before this access review is Review. This list can contain entitlements, account groups, roles, or identities based on the access review type and the default settings of IdentityIQ.

See "Access Review - Common Information" on page 1 for common terms and detailed information on access reviews.

Access Review - Common Information

This section provides information on the common access review information. This information is displayed differently for the different access review types, if it is available. This section also contains electronic signature information, if that feature is enabled.

Note: This information is displayed on the information panel.

Due: the date on which this access review is due.

Owner: the identity to whom this access review is assigned.

Phase: the phase at this time and the date when this phase ends.

Revocations: number reflects the fraction of revocation requests completed for this access review a compared to the total number requested. The revocation competition status is updated at an interval specified during the deployment of IdentityIQ. By default this is performed daily.

Tags: listed are any tags assigned to the certification when the certification was scheduled. Tags are used to classify certifications for searching and reporting purposes.

Reviews: you might not be able to sign off an access review until all subordinate reviews are complete, based on how this certification was scheduled. Click **Additional Reviews** in the status panel to view the subordinate reviews associated with the one displayed. Click a subordinate access review to display the Access Review Decision page. See "Subordinate Access Reviews" on page 16.

A completion notice displays in the Access Review Information panel when all items and subordinate access reviews are in a complete state. Before IdentityIQ recognizes an access review as complete, you must click **Sign Off** and verify that certification is complete on the Sign off Access Review screen. Additional sign off information is required if your installation is configured to require an electronic signature.

Subordinate Access Reviews

Subordinate access review are any access reviews that must be completed before the top-level certification can be considered completed. Examples of subordinate access reviews can include any groups of identities that you reassign, or any lower-level, subordinate, manager access reviews. Lower-level manager access reviews can be created when Manager Certifications are scheduled and can be required as part of that process.

Subordinate access reviews are not displayed as part of the access review list and do not show as part of the completion status for this access review. When specified, subordinate access reviews must be in a complete state before the top-level certification can be signed off.

The **Access Reviews** link displays with the Access Review Decision page if subordinate access reviews exist. Click **Access Reviews** to expand a table containing the following information:

Table 1—Certification Report - Subordinate Certification Descriptions

Column	Description
Name	The name and descriptive information about the top-level certification.
Owner	The current owner of the subordinate access review requests.
Percent Complete	The percentage of the subordinate access review that was acted upon and is in a complete state.
Open	The number of subordinate items that are still in the open state.
Completed	The number of subordinate items that are in the completed state.
Delegated	The number of subordinate items that the current owner delegated to different users.

Column	Description
Action	Click an icon to specify an action to take on the subordinate certification. **Return** — return the subordinate access review items to the review that generated the items and delete the subordinate access review. **Email** — generate an email to send to the owner of the original access review. **Forward** — forward the subordinate access review to a different, qualified certifier.

Access Review Decisions Tab- Access Review Types

The information displayed in the access review decisions tabs is dependent on the type of access review you are working with and the configuration of your implementation of IdentityIQ. Go to the appropriate section for documentation on the different views.

The access review decision panels can also contain informational messages or icons for the items displayed.

> **Note:** If you are performing an Application Owner access review, only information pertaining to the applications included in the access review are displayed for each identity in the list.

> **Note:** If you are performing a Role Membership access review, only information pertaining to the roles included in the access review are displayed for each identity in the list.

- **Target List** — Used for Targeted certifications. This view displays a flattened list of all of the items that are part of this access review as defined at run time. By default, these items are grouped by the identity with which they are associated.

  - "Targeted Certifications" on page 21

- **Identity List** – Used for Manager, Application Owner, and Advanced access reviews. This view displays a flattened list of all of the individual entitlements, roles, and policy violations that are part of this access review. By default, these items are grouped by the identity with which they are associated. "Access Review Details - Identity List" on page 25

- **Object List** – Used for Role Membership or Entitlement Owner access reviews. This view displays either a flattened list of the identities to whom the roles contained in the access review have been assigned or a list of the entitlements included in this access review.

  - "Role Membership and Entitlement Owner Access Reviews" on page 29.

- **Account Group List** – Used for account group access reviews. This view displays a flattened list all of the account groups/application objects that are part of this access review. "Account Group Membership and Account Group Permission Access Reviews" on page 37.

- **Role Composition List** – Used for role composition access reviews. This view displays a flattened list of all the roles that are part of this access review.

  - "Role Composition Access Reviews" on page 33.

My Access Reviews Page

Use this page to view the access reviews assigned to you. The number displayed in the circle next to the access review title indicates the number of access reviews you have. The My Access Review page contains a description of the access review along with the following information:

Note: **Completed access reviews are visible unless archive certification is configured. Access reviews in the Staging phase are also displayed on this page.**

Table 2—My Access Review Page Listings Descriptions

Item	Description
Percentage Completed	The percentage of the access review completed. For example, 46% (6 of 13) means you have certified 6 of the 13 items on the list, or 46% of the total number. Access reviews that are complete, but unsigned are marked with an exclamation point icon.
Due	The due date is the expiration date for this access review or the date and time when the access review was signed off. The due date is used to determine when reminder and escalation rules are sent. The expiration date is the duration of the active phase plus the duration of the challenge phase, if the challenge function is active. If an expiration date is not set this field is marked N/A until the access review is signed off.
Completed	Lists the actions that are completed.
Requested By	The person who scheduled the certification.
e-Signed	**Note: This item is hidden by default. It does not display if the access review has not been e-signed or does not require an e-Signature.** A check-mark icon indicates that an electronic signature exists for the access review.
Phase	The current phase of the access review process. For detailed descriptions of the phases, refer to the "Types of Certification" on page 6.
Tags	Create tags to classify access reviews for searching and reporting. Tags are optionally assigned when certifications are scheduled. This column is empty if tags were not assigned.
Forward Icon	**Note: This item is not available for all access reviews. The availability Forward depends-on individual certification and configuration settings.** Click the **Forward** icon to forward the access review and all included items to a different IdentityIQ user or workgroup. You have the option to add comments.
Start - Continue - View	The option that displays is based on the status of the access review. Start — Select **Start** to begin working on the access review. Continue — Select **Continue** to move to the next page or step. View — Select **View** to view a completed and signed-off access review.

Display Options

Display options for this page include:

- Sort by — Select this option to display access reviews by items such as, Due Date, Phase, Requested By, or % complete.
- Sort order icon — Reverse the sort order
- Show — Select the number of items to display per page

Features

> **Note:**   **You cannot take action on yourself unless that function is enabled during configuration.**

You can perform the following actions from the My Access Review page:

- Details — Click **Start**, **Continue**, or **View** on an access review to display the Access Review Details page. See "Access Review Page Overview" on page 15
- Forward — Click the Forward icon for an access review to forward an access review request to a different IdentityIQ user or workgroup. When you forward an access review, it is removed from your list and does not reflect in your risk score statistics. Owner history and all comments are maintained with the work item.

> **Note:**   **The Forward feature is not available for all access reviews. This feature is dependent on individual certification and configuration settings.**

IdentitiyIQ User Guide

Chapter 3: Targeted Certifications

The access review might look different in your instance of IdentityIQ depending on the configuration and the options selected when the certification was defined.

For detailed information on certifications and access reviews, see "Certification Overview" on page 11.

For detailed information on completing an access review, see "Access Review Decisions/Operations" on page 41.

Access Review Details - Targeted

This page is comprised of all roles, entitlements and policy violations that are part of this access review.

The page contains three tabs:
- Important — Contains items that require immediate attention, such as policy violations
- Open — All of the other access review items that have yet to be acted upon
- Review — The items on which a decision has been made

By default the page opens with the Important tab displayed, if there are policy violations that require immediate action.

Targeted Page Features

The following features are available for all of the tabs:
- List icon —click the icon to display a list of the identities that make up the access review.
- Download to CSV icon — click the icon to download the access review list to a CSV file.
- Information icon —click the information icon to get details about the access review, including due date, phase, and subordinate access reviews.
- Columns —add, remove, or rearrange the columns displayed on the page.
- Group By — rearrange the sort order of items on the page.
- Filter —use a filter to limit the items displayed.

  Note: **The recommendations icon is only displayed If SailPoint IdentityAI was purchased and activated for your installation of IdentityIQ. See the SailPoint** *IdentityAI Implementation Guide* **for more information.**

- Recommendations — display the Decision Recommendation popup
- Bulk Decision button —make the same decision for multiple items. If only one action is applicable, that action appears on the button.
- Bulk select/deselect — click the box on the header line and choose to select or deselect multiple items.

Important Tab

The Important tab contains the following information:

  Note: **The Important tab is not displayed if no urgent issues exist.**

Table 1— Targeted - Important Tab

Column	Description
Policy Name	Name of the policy being violated.
Policy Description	Description of the policy being violated.
Rule	Specific rule that is being broken to cause the violation of the policy.
Owner	Owner of the policy.
Identity	Identity that is in violation.

Use the Decision column to **Allow** the violation, or click the menu icon to display additional options; Delegate, Comment, History, Details.

Delegated items are still part of this access review and must be acted upon before it is complete.

Use **Reassign** to reassign the policy violation decision to another user.

The Open Tab

The Open tab contains the following information by default. You can configure which columns appear on the Open tab by clicking the Columns button and adding, removing, or rearranging columns as needed.

Table 2— Targeted - Open Tab

Column	Description
Type	Role, entitlement, or account.
Display Name	The item name as it appears throughout the product.
Description	The description associated with the item.
Classifications	This column appears only if "Show Classifications" was enabled for the certification. If an entitlement has classification data associated with it, to flag that the permission gives access to potentially sensitive or otherwise protected data, a classification icon appears in this column. Click the icon to see details about the classification.
Application	The application with which the item is associated.
Account Name	The account name for the application with which the item is associated and the account status, enabled or disabled.
Identity	The identity associated with the role, entitlement, or account.

Table 3— Targeted - Accounts Only List - Open Tab

Column	Description
Type	Role, entitlement, or account.
Display Name	The item name as it appears throughout the product.
Description	The description associated with the item.

Table 3— Targeted - Accounts Only List - Open Tab

Column	Description
Classifications	This column appears only if "Show Classifications" was enabled for the certification. If an entitlement has classification data associated with it, to flag that the permission gives access to potentially sensitive or otherwise protected data, a classification icon appears in this column. Click the icon to see details about the classification.
Application	The application with which the item is associated.
Account Name	The account name for the application with which the item is associated and the account status, enabled or disabled.
Identity	The identity associated with the role, entitlement, or account.

Use the Decision column to **Approve** or **Revoke** the item, or click the menu icon to display additional options; Allow, Delegate, Revoke Account, Comment, History, Account Details.

Click the recommendation icon for details about the recommendation. The recommendations icon is only displayed If SailPoint IdentityAI was purchased and activated for your installation of IdentityIQ. See the SailPoint IdentityAI Implementation Guide for more information.

Revoking an account affects all role or entitlements with which it is associated.

Delegated items are still part of this access review and must be acted upon before it is complete.

Use the **Bulk Decisions** to make decision for multiple items or reassign items to another decision maker.

Review Tab

The Review tab contains all of the items upon which a decision has been made. Click the menu icon in the Decision column to change or undo a decision.

Click the automatic approval icon for details about the approval. The the automatic approval icon is only displayed If SailPoint IdentityAI was purchased and activated for your installation of IdentityIQ. See the SailPoint *IdentityAI Implementation Guide* for more information.

How To Perform a Targeted Access Review

Note: **The options available in an access review are dependent on the configuration of IdentityIQ and the option defined when the certification was scheduled.**

Note: **Use Bulk Decisions to reassign items to another decision maker.**

1. Access the targeted access review from the My Access Reviews page or directly from your Home page.

2. Select items individually and select an action in the Decision column.
   — OR —
   Select multiple items and select an action from Bulk Decision list.

3. Click **Save Decisions** to move the completed items to the Review tab.

   Note: **Automatically approved items are displayed on the Review tab where you can accept the approval or change the decision as needed.**

4. Review your decisions on the Review tab and make any required changes.

5.   When all decisions have been made, click Sign-Off Decision to display the Sign Off on Certification dialog.

Chapter 4: Manager, Application Owner, Advance Certifications

Manager, Application Owner, and Advanced Certifications share a common user interface. The access review might look different in your instance of IdentityIQ depending on the configuration and the options selected when the certification was defined. These are all identity list - type certifications.

For detailed information on certifications and access reviews, see "Certification Overview" on page 11.

For detailed information on completing an access review, see "Access Review Decisions/Operations" on page 41.

Access Review Details - Identity List

The identity list is composed of all identities containing roles, entitlements and policy violations that are part of this access review.

The identity list page contains three tabs:

- Important — Contains items that require immediate attention, such as policy violations
- Open — All of the other access review items that have yet to be acted upon
- Review — The items on which a decision has been made

By default the page opens with the Important tab displayed, if there are policy violations that require immediate action.

Identity List Page Features

The following features are available for all of the tabs:

- Identity list icon —click the icon to display a list of the identities that make up the access review.
- Download to CSV icon — click the icon to download the access review list to a CSV file.
- Information icon —click the information icon to get details about the access review, including due date, phase, and subordinate access reviews.
- Columns —Add, remove, or rearrange the columns displayed on the page.
- Group By —Rearrange the sort order of items on the page.
- Filter —Use a filter to limit the items displayed.

  Note: **The recommendations icon is only displayed If SailPoint IdentityAI was purchased and activated for your installation of IdentityIQ. See the SailPoint *IdentityAI Implementation Guide* for more information.**

- Recommendations — display the Decision Recommendation popup
- Bulk Decision button —make the same decision for multiple items. If only one action is applicable, that action appears on the button.
- Bulk select/deselect — click the box on the header line and choose to select or deselect multiple items.

Important Tab

The Important tab contains the following information:

Note: **The Important tab is not displayed if no violations exist.**

Table 1— Identity List - Important Tab

Column	Description
First Name	The first name associated with the identity that requires access review.
Last Name	The last name associated with the identity that requires access review.
Policy Name	The policy in violation.
Policy Description	Description of the policy.
Rule	The rule from the policy in violation.
Owner	The owner of the policy.

Use the Decision column to **Allow** the violation, or click the menu icon to display additional options; Delegate, Comment, History, Details.

Delegated items are still part of this access review and must be acted upon before it is complete.

Use **Reassign** to reassign the policy violation decision to another user.

The Open Tab

The Open tab contains the following information:

Table 2— Identity List - Open Tab

Column	Description
First Name	The first name associated with the identity that requires access review.
Last Name	The last name associated with the identity that requires access review.
Type	The type of item being certified, Role or Entitlement.
Display Name	The item name as it appears throughout the product.
Description	The description associated with the item.
Classifications	This column appears only if "Show Classifications" was enabled for the certification. If an entitlement has classification data associated with it, to flag that the permission gives access to potentially sensitive or otherwise protected data, a classification icon appears in this column. Click the icon to see details about the classification.
Application	The application with which the item is associated.
Account Name	The account name for the application with which the item is associated and the account status, enabled or disabled.

Use the Decision column to **Approve** or **Revoke** the item, or click the menu icon to display additional options; Allow, Delegate, Revoke Account, Comment, History, Account Details.

Click the recommendation icon for details about the recommendation. The recommendations icon is only displayed If SailPoint IdentityAI was purchased and activated for your installation of IdentityIQ. See the SailPoint *IdentityAI Implementation Guide* for more information.

Revoking an account affects all role or entitlements with which it is associated.

Delegated items are still part of this access review and must be acted upon before it is complete.

Use the **Bulk Decisions** to make decision for multiple items or reassign items to another decision maker.

Review Tab

The Review tab contains all of the items upon which a decision has been made. Click the menu icon in the Decision column to change or undo a decision.

Click the automatic approval icon for details about the approval. The the automatic approval icon is only displayed If SailPoint IdentityAI was purchased and activated for your installation of IdentityIQ. See the SailPoint *IdentityAI Implementation Guide* for more information.

How To Perform an Identity List Access Review

Note: The options available in an access review are dependent on the configuration of IdentityIQ and the option defined when the certification was scheduled.

Note: Use Bulk Decisions to reassign items to another decision maker.

1.   Access the identity list access review from the My Access Reviews page or directly from your Home page.

2. Select items individually and select an action in the Decision column.
   — **OR** —

   Select multiple items and select an action from Bulk Decision list.

3. Click **Save Decisions** to move the completed items to the Review tab.

   Note: **Automatically approved items are displayed on the Review tab where you can accept the approval or change the decision as needed.**

4. Review your decisions on the Review tab and make any required changes.

5. When all decisions have been made, click Sign-Off Decision to display the Sign Off on Certification dialog.

Chapter 5: Role Membership and Entitlement Owner Access Reviews

Role Membership and Entitlement Owner access reviews share a common user interface. The access review might look different in your instance of IdentityIQ depending on the configuration and the options selected when the certification was defined. These are all object list - type certifications.

For detailed information on certifications and access reviews, see "Certification OverviewIdentityIQ enables you to automate the review and approval of identity access privileges. IdentityIQ collects fine-grained access or entitlement data and formats the information into reports, which are sent to the appropriate reviewers as access reviews. Certifications consist of multiple access reviews. For example, you can schedule a Manager Certification with individual access reviews that require approvers to take action. System Administrators and Certification Administrators can take action on all access review items whether they own them or not." on page 11.

For detailed information on completing an access review, see "Access Review Decisions/Operations" on page 41.

Access Review Details - Object List

The object list is composed of all roles or entitlements that are part of this access review.

The object list page contains three tabs:
- Important — Contains items that require immediate attention, such as returned delegations
- Open — All of the other access review items that have yet to be acted upon
- Review — The items on which a decision has been made

By default the page opens with the Important tab displayed, if there are issues that require immediate action.

Object List Page Features

The following features are available for all of the tabs:

- Object list icon —click the icon to display a list of the items that make up the access review.
- Download to CSV icon — click the icon to download the access review list to a CSV file.
- Information icon —click the information icon to get details about the access review, including due date, owner, phase, number of completed items and revocations.
- Columns —Add, remove, or rearrange the columns displayed on the page.
- Group By —Rearrange the sort order of items on the page.
- Filter —Use a filter to limit the items displayed.

   Note: **The recommendations icon is only displayed If SailPoint IdentityAI was purchased and activated for your installation of IdentityIQ. See the SailPoint *IdentityAI Implementation Guide* for more information. Recommendations are not available on Entitlement Owner Certifications.**

- Recommendations — display the Decision Recommendation popup
- Bulk Decision button —make the same decision for multiple items. If only one action is applicable, that action appears on the button.
- Bulk select/deselect — click the box on the header line and choose to select or deselect multiple items.

Important Tab

The Important tab contains the following information:

   Note: **The Important tab is not displayed if no urgent issues exist.**

Table 1— Entitlement List - Important Tab

Column	Description
First Name	The first name associated with the item that requires access review.
Last Name	The last name associated with the item that requires access review.
Display Name	The entitlement named used throughout IdentityIQ.
Attribute	The attribute with which the entitlement is associated.
Account Name	The name of the account with which the entitlement is associated.
Description	Description of the entitlement.
Return Comment	Any comments associated with this item.
Decision	The decision made by the reviewer to whom this item was delegated, or by the user from whom it was revoked.

Table 2— Role Membership List - Important Tab

Column	Description
First Name	The first name associated with the item that requires access review.
Last Name	The last name associated with the item that requires access review.
Role	The name of the role.

Table 2— Role Membership List - Important Tab

Column	Description
Description	Description of the role.
Classifications	For Role Membership reviews only. This column appears if "Show Classifications" was enabled for the certification. If an entitlement has classification data associated with it, to flag that the permission gives access to potentially sensitive or otherwise protected data, a classification icon appears in this column. Click the icon to see details about the classification.
Return Comment	Comments from the reviewer to whom the decision was delegated.
Role Application	The application with which the role is associated.
Decision	The decision made by the reviewer to whom the decision was delegated.

Delegated items are still part of this access review and must be acted upon before it is complete.

Use **Reassign** to reassign the policy violation decision to another user.

The Open Tab

The Open tab contains the following information:

Table 3— Entitlement List - Open Tab

Column	Description
First Name	The first name associated with the item that requires access review.
Last Name	The last name associated with the item that requires access review.
Display Name	The entitlement named used throughout IdentityIQ.
Attribute	The attribute with which the entitlement is associated.
Account Name	The name of the account with which the entitlement is associated.
Description	Description of the entitlement.

Table 4— Role Membership List - Open Tab

Column	Description
First Name	The first name associated with the item that requires access review.
Last Name	The last name associated with the item that requires access review.
Role	The name of the role.
Description	Description of the role.
Classifications	For Role Membership reviews only. This column appears if "Show Classifications" was enabled for the certification. If an entitlement has classification data associated with it, to flag that the permission gives access to potentially sensitive or otherwise protected data, a classification icon appears in this column. Click the icon to see details about the classification.
Return Comment	Comments from the reviewer to whom the decision was delegated.

Use the Decision column to **Approve** or **Revoke** the item, or click the menu icon to display additional options; Allow, Delegate, Revoke Account, Comment, History, Account Details.

Click the recommendation icon for details about the recommendation. The recommendations icon is only displayed If SailPoint IdentityAI was purchased and activated for your installation of IdentityIQ. See the SailPoint *IdentityAI Implementation Guide* for more information. Recommendations are not available on Entitlement Owner certifications.

Revoking an account affects all role or entitlements with which it is associated.

Delegated items are still part of this access review and must be acted upon before it is complete.

Use the **Bulk Decisions** to make decision for multiple items or reassign items to another decision maker.

Review Tab

The Review tab contains all of the items upon which a decision has been made. Click the menu icon in the Decision column to change or undo a decision.

Click the automatic approval icon for details about the approval. The the automatic approval icon is only displayed If SailPoint IdentityAI was purchased and activated for your installation of IdentityIQ. See the SailPoint *IdentityAI Implementation Guide* for more information.

How to Perform an Object List Access Review

Note: **The options available in an access review are dependent on the configuration of IdentityIQ and the option defined when the certification was scheduled.**

Note: **Use Bulk Decisions to reassign items to another decision maker.**

1. Access the object list details from the My Access Reviews page or directly from your Home page.

2. Select items individually and select an action in the Decision column.
    — OR —

    Select multiple items and select an action from Bulk Decision list.

3. Click **Save Decisions** to move the completed items to the Review tab.

    Note: **Automatically approved items are displayed on the Review tab where you can accept the approval or change the decision as needed.**

4. Review your decisions on the Review tab and make any required changes.

5. When all decisions have been made, click Sign-Off Decision to display the Sign Off on Certification dialog.

Chapter 6: Role Composition Access Reviews

The list is composed of all of the roles that make up this access review. This list is only available for Role Composition access reviews. The access review might look different in your instance of IdentityIQ depending on the configuration and the options selected when the certification was defined. These are all role composition list - type certifications.

For detailed information on certifications and access reviews, see "Certification OverviewIdentityIQ enables you to automate the review and approval of identity access privileges. IdentityIQ collects fine-grained access or entitlement data and formats the information into reports, which are sent to the appropriate reviewers as access reviews. Certifications consist of multiple access reviews. For example, you can schedule a Manager Certification with individual access reviews that require approvers to take action. System Administrators and Certification Administrators can take action on all access review items whether they own them or not." on page 11.

For detailed information on completing an access review, see "Access Review Decisions/Operations" on page 41.

Access Review Details - Role Composition List

The role composition list is composed of all roles that are part of this access review.

The object list page contains three tabs:
- Important — Contains items that require immediate attention, such as returned delegations
- Open — All of the other access review items that have yet to be acted upon
- Review — The items on which a decision has been made

By default the page opens with the Important tab displayed, if there are issues that require immediate action.

Object List Page Features

The following features are available for all of the tabs:

- Object list icon —click the icon to display a list of the items that make up the access review.
- Download to CSV icon — click the icon to download the access review list to a CSV file.
- Information icon —click the information icon to get details about the access review, including due date, owner, phase, number of completed items and revocations.
- Columns —Add, remove, or rearrange the columns displayed on the page.
- Group By —Rearrange the sort order of items on the page.
- Filter —Use a filter to limit the items displayed.
- Bulk Decision button —make the same decision for multiple items. If only one action is applicable, that action appears on the button.
- Bulk select/deselect — click the box on the header line and choose to select or deselect multiple items.

Important Tab

The Important tab contains the following information:

Note: **The Important tab is not displayed if no urgent issues exist.**

Table 1— Role Composition List - Important Tab

Column	Description
Role	The name of the role with which this item is associated.
Name	The name of the line item being reviewed.
Type	The type of role or entitlement profile.
Description	Description of the role.
Application	The application associated with this item, if appropriate.
Return Comments	Any comments associated with this item.
Decision	The decision made by the reviewer to whom this item was delegated.

Delegated items are still part of this access review and must be acted upon before it is complete.

Use **Reassign** to reassign the policy violation decision to another user.

The Open Tab

The Open tab contains the following information:

Table 2— Role Composition List - Open Tab

Column	Description
Name	The name of the role or the individual line items contained within.
Type	The type of role or entitlement profile.

Table 2— Role Composition List - Open Tab

Column	Description
Description	Description of the role.
Application	The application associated with this item, if appropriate.

Use the Decision column to **Approve** or **Revoke** the item, or click the menu icon to display additional options; Allow, Delegate, Revoke Account, Comment, History, Account Details.

Revoking an account affects all role or entitlements with which it is associated.

Delegated items are still part of this access review and must be acted upon before it is complete.

Use the **Bulk Decisions** to make decision for multiple items or reassign items to another decision maker.

Review Tab

The Review tab contains all of the items upon which a decision has been made. Click the menu icon in the Decision column to change or undo a decision.

How to Perform a Role Composition Access Review

Note:	The options available in an access review are dependent on the configuration of IdentityIQ and the option defined when the certification was scheduled.

Note:	Use Bulk Decisions to reassign items to another decision maker.

1.	Access the access review details page from the My Access Reviews page or directly from your Home page.

2.	Click an item to display the detailed role information.

3.	Take action on individual items.
	— OR —

	Use the select boxes and select an action from Bulk Decision list.

4.	Click **Save Decisions**.

5.	When all decisions have been made, click **Sign-Off Decisions** to display the Sign Off on Certification dialog.

Chapter 7: Account Group Membership and Account Group Permission Access Reviews

The access review might look different in your instance of IdentityIQ depending on the configuration and the options selected when the certification was defined. These are all account group list - type certifications.

For detailed information on certifications and access reviews, see "Certification OverviewIdentityIQ enables you to automate the review and approval of identity access privileges. IdentityIQ collects fine-grained access or entitlement data and formats the information into reports, which are sent to the appropriate reviewers as access reviews. Certifications consist of multiple access reviews. For example, you can schedule a Manager Certification with individual access reviews that require approvers to take action. System Administrators and Certification Administrators can take action on all access review items whether they own them or not." on page 11.

For detailed information on completing an access review, see "Access Review Decisions/Operations" on page 41.

Access Review Details - Account Group List

The list is composed of all of the account groups, application objects, that make up this access review.

The object list page contains three tabs:
- Important — Contains items that require immediate attention, such as returned delegations.
- Open — All of the other access review items that have yet to be acted upon.
- Review — The items on which a decision has been made.

By default the page opens with the Important tab displayed, if there are issues that require immediate action.

Object List Page Features

The following features are available for all of the tabs:

- Object list icon —click the icon to display a list of the items that make up the access review.
- Download to CSV icon — click the icon to download the access review list to a CSV file.
- Information icon —click the information icon to get details about the access review, including due date, owner, phase, number of completed items and revocations.
- Columns —Add, remove, or rearrange the columns displayed on the page.
- Group By —Rearrange the sort order of items on the page.
- Filter —Use a filter to limit the items displayed.
- Bulk Decision button —make the same decision for multiple items. If only one action is applicable, that action appears on the button.
- Bulk select/deselect — click the box on the header line and choose to select or deselect multiple items.

Important Tab

The Important tab contains the following information:

Note: **The Important tab is not displayed if no urgent issues exist.**

Table 1— Account Group Permissions List - Important Tab

Column	Description
Account Group	The account group name.
Type	The type of the account group.
Description	Description of the account group.
Attribute	The attribute associated with this account group.
Entitlements	Any entitlements associated with the account group.
Return Comment	Any comments associated with this item.
Decision	The decision made by the reviewer to whom this item was delegated.

Table 2— Account Group Membership List - Important Tab

Column	Description
First Name	The first name of the account group member.
Last Name	The last name of the account group member.
Type	The type of the account group.
Description	Description of the account group.
Return Comments	Any comments associated with this item.
Decision	The decision made by the reviewer to whom this item was delegated.

Delegated items are still part of this access review and must be acted upon before it is complete.

Use **Reassign** to reassign the policy violation decision to another user.

The Open Tab

The Open tab contains the following information:

Table 3— Account Group Permissions List - Open Tab

Column	Description
Account Group	The account group name.
Type	The type of the account group.
Description	Description of the account group.
Attribute	The attribute associated with this account group.
Entitlements	Any entitlements associated with the account group.

Table 4— Account Group Membership List - Open Tab

Column	Description
First Name	The first name of the account group member.
Last Name	The last name of the account group member.
Type	The type of the account group.
Account	The name of the account associated with this member.
Description	Description of the account group.

Use the Decision column to **Approve** or **Revoke** the item, or click the menu icon to display additional options; Allow, Delegate, Revoke Account, Comment, History, Account Details.

Revoking an account affects all role or entitlements with which it is associated.

Delegated items are still part of this access review and must be acted upon before it is complete.

Use the **Bulk Decisions** to make decision for multiple items or reassign items to another decision maker.

Review Tab

The Review tab contains all of the items upon which a decision has been made. Click the menu icon in the Decision column to change or undo a decision.

How to Perform an Account Group Access Review

> **Note:** The options available in an access review are dependent on the configuration of IdentityIQ and the option defined when the certification was scheduled.

> **Note:** Use Bulk Decisions to reassign items to another decision maker.

1. Access the access review details page from the My Access Reviews page or directly from your Home page.

2. Take action on individual items.
   — OR —

   Use the select boxes and select an action from Bulk Decision list.

3. Click **Save Decisions**.

4. When all decisions have been made, click **Sign-Off** Decision to display the Sign Off on Certification dialog.

Chapter 8: Access Review Decisions/Operations

> **Note:** The terms account group and application object are use interchangeably in this document but have the same meaning. Some applications can have multiple application objects. An account group can be the name of one of those objects.

There are many ways to move through the IdentityIQ application. As you become familiar with IdentityIQ, you can configure the product to fit the functions of your job. To take action, you must be the owner or delegated approver of an access review. You might be able to view another user's access review; however, the reviews are read-only files.

> **Note:** System Administrators and Certification Administrators can take action on all access review items whether they own the certification or not.

Basic Access Review Procedure

Access Reviews are performed from the Access Review Page Overview page.

1. Go to your My Access Review page.

2. Perform one of the following actions on each item included in the Access Review Request:

   > **Note:** Not all of the decision options are available at all times.

   - Reassign — See "Reassign Access Reviews" on page 42.

   - Approve — See "Approve Access Reviews" on page 43.

   - Delegate — See "Delegate Access Reviews" on page 43.

   - Allow Exception — See "Allow Exceptions on Access Reviews" on page 44.

   - Revoke or Edit Access — See "Revoke or Edit Access From Access Reviews" on page 44.

   - Revoke Account — See "Revoke an Account on Access Reviews" on page 45.

   - Allow Violation — See "Allow Policy Violations on Access Reviews" on page 46.

3. Save your changes. Any decision made on the Access Review Details page or the Decisions tab must be saved before to moving to a different page. A warning prompts for any unsaved changes.

   Decisions are not committed at this point, however, and can still be changed before the access review is signed off on.

   > **Note:** Changing the decisions might revoke one or more line item delegations. Any changes made during the delegation will be lost.

4. Sign off a periodic certification task before it is overdue.

   > **Note:** All items must be in the complete state before the sign off option is available.
   >
   You must sign off a periodic certification before it is considered complete. Click **Sign Off** on the Access Review Details page and select **Finish** on the Sign Off Access Review screen.

If the challenge period for revocations is active, you cannot sign off an access review until one of the following conditions is met:

- All items are complete and the challenge period is not active or no revocation decisions were made.

- The access review is in the challenge phase and all items are completed and any revocation decisions have progressed through the challenge procedure.

- The challenge period has expired.

5. OPTIONAL: Provide password to complete the electronic signature. Electronic signature requirements are configured when the certification is scheduled. See "Behavior Fields" on page 68
Use the same credentials for the electronic signature that you use to sign in to the product.

Access Review Decisions

Perform one of the following actions on each item included in the Access Review Request:

Note: **Not all of the decision options are available at all times.**

- Reassign — See "Reassign Access Reviews" on page 42.
- Approve — See "Approve Access Reviews" on page 43.
- Delegate — See "Delegate Access Reviews" on page 43.
- Allow Exception — See "Allow Exceptions on Access Reviews" on page 44.
- Revoke or Edit Access — See "Revoke or Edit Access From Access Reviews" on page 44.
- Revoke Account — See "Revoke an Account on Access Reviews" on page 45.
- Allow Violation — See "Allow Policy Violations on Access Reviews" on page 46.

Reassign Access Reviews

You can reassign items individually or use:

- Bulk reassignment to reduce access review lists. For example, if you are the assigned approver of an application with thousands of identities, you can use this feature to reassign identities by department or manager.
- Automatic reassignment or forwarding of all access reviews assigned to you. You can use the Forwarding User field on the Edit Preferences page. If you select a forwarding user, all work items including access review requests are sent to that user.

When you choose to reassign you will see the Reassign Items dialog.

Enter the following information in the reassignment dialog.

- **Recipient** — type the full name of the approver to whom you are reassigning this work item. The recipient can be an identity or a workgroup. Typing the first few letters of a name displays a pop-up menu of IdentityIQ users and workgroups with names containing that letter string. Click the arrow next to the field to display all users.
— OR —

Select an assignee from the drop-down menu. The drop-down menu can contain options such as assign to self, assign to manager, or assign to application owner.

- **Description** — (optional) a brief description of the item being reassigned.

- **Comment** — (optional) any additional information needed.

Click **Reassign** to reassign the item and return to the Access Review Details page.

The Percentage complete bar is updated to show the changes and the selected items are removed from the list and do not show as part of the completion status for this access review. If configured, all reassigned items must be acted upon before you can sign-off a periodic certification.

Approve Access Reviews

You cannot approve policy violations. Warning messages are displayed if you attempt to include policy violations when performing an approval.

If provisioning is enabled from the access review pages and you approve a role that contains required roles to which the identity does not have access, a dialog displays enabling you to request provisioning for those roles. If you perform a bulk approval, this function is overwritten and the roles are approved in their current state.

If you perform bulk approval and the access review has missing roles, you do not have the option to provision required roles. The provisioning function is only available if you approve roles individually and provisioning is enabled for this access review.

If the provisioning dialog displays, review the missing information and make a provisioning decision.

If you choose to request that the missing roles be added, you must select a recipient for the request and click **Provision Required Roles** again. The recipient you specify is used if automatic provisioning is not configured or there is no default remediator for the application. Or click **Do Not Provision** and return to the access review page.

When you perform an approve at the top level you are approving all of the items that are included in the identity, role, entitlement, or account group/application object. Access Reviews performed at this level are logged for auditing purposes.

Delegate Access Reviews

Delegation can be performed automatically based on rules specified when the certification request is generated. Items delegated automatically display in the access review details and behave exactly like items delegated manually.

The Enable Line Item Delegation option must be selected when the certification was created to delegate certification items from the Access Review Details page.

Type the following information in the **Delegate Access Review** dialog.

- **Recipient** — type the full name of the approver to whom you are delegating this work item. The recipient can be an identity or a workgroup. Typing the first few letters of a name displays a pop-up menu of IdentityIQ users and workgroups with names containing that letter string.

- **Description** — a description of the work item being delegated. You can edit the description as required.

- **Comment** — (optional) any additional information needed for this delegation.

Changing the decisions may revoke one or more line item delegations. Any changes made during the delegation that be lost.

You cannot delegate account groups from the account group list.

When you delegate at the top level you are also delegating all of the items that are included in the identity or role.

Allow Exceptions on Access Reviews

> **Note:** **This option is only available if it was turned on in the global settings at the time of your configuration.**

Use **Allow Exception** to put an expiration date on access to a particular entitlement, role, or account group. For example, if one employee must temporarily assume the duties of another during a vacation, you can allow them access to that role for the length of the vacation.

Decisions made in access reviews are shown on the Policy Violations page for the affected policy violation.

Allow exceptions on individual items that make up the identity.

Type the following information in the **Allow Exception** dialog.

- **Expiration** — manually type an expiration date, or click the icon and select a date.
  A 4-digit year is required if you type the date manually. For example, mm/dd/yyyy.

- **Comment** — (optional) any additional information needed for this exception.

Revoke or Edit Access From Access Reviews

This section information on the follow:

- Request the removal of an identity access to a specified role or entitlement
- Remove a permission of member from an account group
- Remove access to a managed entitlement from an identity
- Remove a profile or included role from a role
- Edit the values of specific entitlement attributes or permission on identity-type access reviews

> **Note:** **Entitlements must be configured on the application to enable editing from the access review pages.**

For revocation on individual roles, if a role contains required or permitted roles that are not used in any other roles for this identity, a dialog displays enabling you to make revocation decision on each of those included roles. By default all included roles, that are not used in other roles for this identity, are marked for removal. If you perform bulk revocation this function is overwritten.

On periodic access reviews, by default, no action is taken on a revocation request until the access review containing this item is signed off or the challenge period expires, if the challenge period is active. This is done to ensure that no entitlement is removed until final confirmation is received from the requestor. This default behavior can be overwritten when the access review schedule is created.

Revocation is done automatically if your provisioning provider is configured for automatic revocation through help ticket generation or if your implementation is configured to work with a help desk solution. Without the automatic configurations, revocations are done manually using a work request assigned to a IdentityIQ user or workgroup. If an access review requires that multiple revocation requests be sent to the same IdentityIQ user or workgroup they are rolled up into one work item.

For identity-type access reviews, the revocation process can also include the challenge and revocation periods. The challenge phase is the period during which all revocation requests can be challenged by the user from whom the role or entitlement is being removed or modified. The revocation phase is the period during which all revocation work must be completed. The revocation phase is entered when an access review is signed off or when the active and challenge phases have ended.

Type the following information in the revocation dialog and click **Revoke**.

> **Note:** **This dialog is not displayed if a default revoker was specified as part of the IdentityIQ configuration.**

- **Recipient** — type the full name of the revoker to whom you are assigning this work item. The recipient can be an identity or a workgroup. Typing the first few letters of a name displays a pop-up menu of IdentityIQ users and workgroups with names containing that letter string.
  If automatic remediation is enabled or a default revoker was specified for the application to which the entitlements are associated, the recipient specified here is overwritten.

- **Comment** — (optional) any additional information needed for this revocation.

- **Edit Revocation Details** — only available if the entitlement is configured for modification. One line displays for each entitlement contained in this revocation request.
  Operation — select the operation to perform, Remove or Modify.
  Attribute — attribute name that the attribute or permission is associated.
  Value — if are modifying the entitlement, select or type the new value.
  Application — application to which the entitlement is associated.
  Account ID — login ID of this identity on the application specified.

Revoke an Account on Access Reviews

When you select **Revoke Account** for one entitlement, all other entitlements associated with the same account for the item being certified are marked for revocation.

On periodic certifications, by default, no action is taken on a revocation request until the certification containing the account is signed off or the challenge period expires, if the challenge period is active. This is done to ensure that no account is removed until final confirmation is received from the requestor. When the certification schedule is created, this default behavior can be overwritten allowing revocation requests to be processed immediately.

Revocation is done automatically if your provisioning provider is configured for automatic revocation through help ticket generation or if your implementation is configured to work with a help desk solution. Without the automatic configurations, revocations are done manually using a work request assigned to a IdentityIQ user or workgroup. If a certification requires that multiple revocation requests be sent to the same IdentityIQ user or workgroup they are rolled up into one work item.

For identity-type certifications, the revocation process can also include the challenge and revocation periods. The challenge phase is the period during which all revocation requests can be challenged by the user from which the account is being removed. The revocation phase is the period during which all revocation work must be completed. The revocation phase is entered when a certification is signed off or when the active and challenge phases have ended.

Respond to a Challenged Revocation

For identity- type certifications, the revocation process can include the challenge and revocation periods. The challenge phase is the period when a user whose role or entitlements are being removed can challenge those revocation requests.

When a revocation request is challenged, the status of the item associated with the revocation request displays as **Challenged**. You must take action on all challenged revocations before a certification is complete.

From the **Challenge Decision** drop-down menu select either **Accept** or **Reject**.

All comments are kept with the certification item and can be viewed below the certification decision information for that item. Click **comments** to view the comments added by the challenger and **accepted/rejected** to view the comments associated with the decision.

Based on your decision one of the following occurs:

- **Reject** — the revocation process proceeds as normal when the certification is signed off or the challenge period ends.

- **Accept** — the item is moved to the open status and you must make another certification decision.

Allow Policy Violations on Access Reviews

Do this to allow an identity to retain conflicting roles, accounts, or entitlements for a specific period of time. For example, if one employee must temporarily assume the duties of another, you can allow them access to a role that creates a policy violation for the length of the vacation.

To display detailed information about the policy, click the violation name on the Decisions tab.

Type the following information in the **Allow Violation** dialog.

- **Expiration** — manually type an expiration date, or click the **"..."** icon and select a date.
  A 4-digit year is required if you type the date manually. For example, mm/dd/yyyy.

- **Comment** — (optional) any additional information needed for this exception.

Chapter 9: How to Complete Access Review Work Items

The following procedures list the steps to complete Access Review work items that were originally assigned to a different approver, but now require you, as a member of the workgroup, or the other members of a workgroup to take action. Access review work items include items that were delegated, reassigned, forwarded, require your approval, or require you to take revocation actions.

- "How to Complete Delegated Access Reviews" on page 47
- "How to Complete Revocation Work Items" on page 48
- "How to Complete Reassigned or Forwarded Access Reviews" on page 49
- "How to Perform Multi-Level Sign Off on Access Reviews" on page 49
- "How to Challenge a Revocation Request" on page 49

How to Complete Delegated Access Reviews

You can complete delegated access reviews items from access reviews that were assigned to a different certifier that the original approver delegated to you. For example, if an employee does work for you but reports to a different manager, that manager might not be familiar with all of the entitlements or roles listed in the employee's Identity Cube.

To display the Manage Work Item page, click a delegation work item.

Required Authorization

To take action on a delegated work item, you must be the owner of that work item.

> **Note:** **A System Administrator or Certification Administrator can also take action on work items.**

Procedure

1. Open a delegated work item.

2. Review the work item information in the Summary section.

3. Review the Comments section for any information associated with this work item. Use the **Add Comment** button to add additional information to the work item.

4. Make an access review decision on each item listed for the identity. See "Access Review Details Page - Decisions Tab" on page 1 for detailed information on access review decisions.

5. Click **Complete** to display the **Completion Comments** dialog and mark the work item as complete.

> **Note:** **If your deployment is configured to require a decision on each item in the work item before it is marked complete and you do not take action on all items in the work item, an alert displays when you attempt to complete a work item.**

Optional - Delegation Review

If the access review was originally configured to require a delegation review, you can perform this review after the delegate completes their portion of the access review. The items awaiting review are listed on the **Important** tab of the access review.

1. In the access review, click the **Important** tab. Delegated items that have been completed and are awaiting review are listed in the **Returned Items** section.

2. To view the comments of the delegated decision maker, click the three-line menu and choose **History**,

3. Click **Agree** to accept the delegated decision; if you don't accept the delegated decision, you can override the delegated decision with any of the available options (Revoke, Revoke Account, Allow, etc.). You can also delegate the line item again.

   Note: **If the identity who originally delegated the work item overrides a delegated decision, an audit shows the delegation of the work item was never assigned.**

How to Complete Revocation Work Items

You can confirm that you have completed the requested revocation. Revocation requests are sent after the access review for the associated item is completed and signed off or when the access review enters the challenge phase, if the challenge period feature is active. This process ensures that nothing is removed until the final decision is made on the access review. When you click **Complete** on this work item, you are stating that you acted on the revocation request.

Required Authorization

You must have authorization on the specified application to perform the required revocation.

   Note: **A System Administrator or Certification Administrator can also take action on work items.**

Procedure

1. Select a revocation work item to display the Manage Work Item page.

2. Review the work item information in the Summary section.

3. Review the Comments section for any information associated with this work item.
   Use the Add Comment button to add additional information to the work item if necessary.

4. Review and perform the operations necessary to revoke the privileges specified.
   Click a line item to view the details of the revocation request for that item.
   The revocation of application privileges is not performed as part of IdentityIQ. The revocation is performed on the specific application from which the entitlements are to be removed. For information on how to remove entitlements, refer to the documentation associated with the specific application

5. If this work item was assigned to a workgroup, use the **Assign Selected Items** button to assign specific revocation requests to members of that workgroup. The name of the workgroup member is displayed in the Assignee column.
   Any member of the workgroup can change the assignee status.

6. Click **Complete** to display the **Completion Comments** dialog and mark the work item as complete.
   — OR —
   If there are multiple revocation requests in the work item, you can select multiple revocations and use the **Mark Revocation Complete** button to mark complete. Alternatively, you can click on the revocation item and complete each item individually.

How to Complete Reassigned or Forwarded Access Reviews

You can reassign or forward access reviews. Reassigned work items are designated as reassigned in the Description columns on pages on which they are displayed. Forwarded work item descriptions maintain the name of the original owner or the name of the application to which the access review applies.

You use the same procedure to complete access reviews that were reassigned or forwarded to you that you use for access reviews that were originally assigned to you. See "Access Review Decisions/Operations" on page 41.

How to Perform Multi-Level Sign Off on Access Reviews

You can perform multi-level sign-off access reviews that require more than one person to review before sign off. Multi-level sign-off access reviews are access reviews that an assigned certifier completed and signed off and require other users to review before the access reviews are complete. When an access review is assigned to you for additional sign off, you receive an email notification and the access review request is sent to you.

You can access the access review request the same way as any other access review, make changes or add comments as required, and click **Sign Off** when you are finished.

After you sign off, the multi-level sign off rule runs again to determine if the access review is complete or if additional sign off actions are required. This process is repeated until the rule determines that no further sign-off actions are required for the access review.

How to Challenge a Revocation Request

The challenge phase is the period when the user whose role or entitlement is being removed, can challenge all revocation requests.

For identity-type access reviews, the revocation process can include the challenge and revocation periods.

If a role or entitlement is removed from your Identity Cube, you are assigned a work item that enables you to accept or challenge the revocation.

To accept the revocation, do not respond to this challenge work item.

To challenge the revocation request, type your reasons for the challenge in the **Reason for Challenge** field and click **Challenge**. Or click **Cancel** to close the work item without taking action.

Chapter 10: Certification Events

Certifications can be configured to run based on events that occur within IdentityIQ. For example, an event-based certification might be configured to run when a manager change is detected for an identity and for that certification request to be sent to the newly assigned manager. The events that trigger the certifications can be configured to meet the needs of your enterprise.

Use the Certification Event tab to configure events within your enterprise to trigger the creation and assignment of certification requests. Event-based certifications are launched when changes are detected during an identity refresh.

To access the Certification Events panel, click the Setup tab and select **Certifications.** On the Certifications page click the **Certification Events** tab. Click an existing certification event to view the details defined when it was created. Click **New Certification Event** to display the certification event configuration panel.

The Certifications Events tab contains the following information:

Table 1—Certifications Events Tab Column Descriptions

Column	Description
Name	The name assigned when the certification event was created. **Note: This name is used to identify the certification event. This name is not displayed in the certifications that are created when this event is triggered.**
Type	The event type associated with this certification event.
Attribute Name	The attribute specified in attribute change type certification events.
Owner	The user that created the event certification.
Disabled	Indicates whether or not the certification event is enabled.

Define a Certification Event

For a list and descriptions of the fields on the Event Certification panel, see Table 2, "Certification Event field descriptions," on page 52. You can also see a field description by placing your cursor on the question mark (?) icon displayed beside each field name.

To schedule a certification from a certifying event, you make decisions on the Basic, Lifecycle, Notifications, and Advanced tabs. The left panel provides a summary and descriptions of the tabs. To move through the scheduling process, select a tab in the Summary panel or click **Next** at the bottom of the page. You do not have to move through the tabs in order.

When a Certification Event is set up, all certifications for that event are listed in the same certification group on the Setup > Certifications page.

> Note: **Event certifications are generated as Identity certifications and are displayed as such. To separate Event certifications from other Identity certifications use the Custom Name and Custom Short name options on the Advanced panel.**

To schedule a non-event certification, see "Certifications Tab" on page 59.

Table 2—Certification Event field descriptions

Field Name	Description
Basic: **These options specify what and when to certify and who is responsible for performing the access reviews.**	
Name	Assign a descriptive name for the event certification. **Note: This name is used to identify the event certification. This name is not displayed in the certification requests that are created when an event is triggered.**
Description	Add a brief description of the certification event.
Event Type	Specify an event-type or rule to associate with the certification. **Create** - launch a certification when a new identity is discovered. **Manager Transfer** - launch a certification when an identity's manager changes. **Attribute Change** - launch a certification when a change is detected for the specified attribute. **Rule** - use a rule to determine when certifications are launched. **Native Change** - launch a certification when a change is detected on a native application. **Alert** - launch a certification when an alert is triggered within your enterprise
Previous Manager Filter	For Manager Transfer event certification types only: Certifications are launched if identities are transferred from the specified manager. If no manager is specified, all managers are included.
New Manager Filter	For Manager Transfer event certification types only: Certifications are launched if identities are transferred to the specified manager. If no manager is specified, all managers are included.
Attribute	For Attribute Change event certifications types only: Select the identity attribute to associate with the event certification. The attribute drop-down list contains all of the standard and extended identity attributes configured in your deployment of IdentityIQ.
Previous Value Filter	For Attribute Change event certification types only: Certifications are launched if the attribute value specified has changed. If no value is specified, all values are included.
New Value Filter	For Attribute Change event certification event types only: Certifications are launched if the attribute value specified was newly assigned. If no value is specified, all values are included.
Rule	For Rule event certification types only: Select the event certification rule used to launch certifications. Rules are created as part of the configuration process of IdentityIQ.
Disabled	Select to specify that a lifecycle event should not be processed.

Table 2—Certification Event field descriptions

Field Name	Description
Included Identities	Specifies which identities to include when detecting this lifecycle event. Select one of the following filter types to narrow your selection: **Match List** — a list of attributes and permissions on selected applications. **Filter** — a custom database query for role creation. **Script** — a custom script for role creation. **Rule** — select an existing rule from the drop-down list. **Note: Click the "..." icon to launch the Rule Editor to make changes to your rules if needed.** **Population** — select an existing population of identities to include.
Certification Name	Specify the name of the certification associated with the certification event.
Certification Owner	Specify the owner of the certification.
Certifiers	Specify the full name of the person or people to be assigned the certification. To display a list of all valid certifiers in the system, type the first few letters of the name and then select a name from the displayed list. **Assign to Manager(s)** - assign to the manager(s) of the identities for whom the certifications are created. You must also enter a default certifier in case some of the identities do not have a manager assigned. **Select Certifier(s) Manually** - manually specify certifiers to whom these event certifications will be assigned.
Included Applications	Specify the applications with the roles and entitlements that should be discovered when generating this certification. If no applications are specified, then all of the applications are included.
Included Access	Include entitlements or Accounts in the certification that are assigned to an identity but are not contained within a defined role.
Include Policy Violations	Include policy violations for each identity in the certification report. If this field is deactivated no policy violations are included.
Include Roles	Include roles assigned to the identity in the certification.
Tags	Specify one or more tags for the certifications. Tags can be used to classify certifications for searching and reporting.
Lifecycle: **These options define the lifecycle of the certification.**	
Active Period Enter Rule	Select a rule to run when the certification enters its active period.
Active Period Duration	Specify the length of the review period during when all decisions required within this certification should be made. During this phase changes can be made to decisions as frequently as needed. You can sign off on a certification in the active stage if no roles or entitlements were revoked or if the challenge period is not active. When you sign off on a certification, it enters the end phase or the revocation phase. To enter the revocation phase, the revocation period must be active and a revocation decision must exist.

Table 2—Certification Event field descriptions

Field Name	Description
Enable Challenge Period	Specify the period when all revocation requests can be challenged by the user whose role or entitlement is being removed. When the challenge phase begins, a work item and email are sent to each user in the certification that the revocation decision affects. The work items contain the details of the revocation request and any comments the requestor adds. The affected user has the duration of the challenge period to accept the loss of access or challenge that decision. You can sign off on a certification in the challenge phase if all challenges are completed and there is no open decision on the certification. When you sign off on a certification, it enters the end phase or the revocation phase. To enter the revocation phase, the revocation period must be active and a revocation decision must exist.
Enable Revocation Period	**Note: If the revocation period is disabled, the certification is not scanned for completed revocations and revocation status might not be accurately reflected throughout the product.** Specify the period when all revocation work should be completed. Revocations can be done automatically or manually. Your provisioning provider must be configured for automatic revocation. Manual revocations use a work request assigned to a IdentityIQ user with the proper authority on the specified application. The revocation phase begins when a certification is signed off or when the active and challenge phases have ended. Revocation activity is monitored to ensure that inappropriate access to roles and entitlements is revoked in a timely manner. Revocation completion status is updated at an interval specified during the deployment of IdentityIQ. By default this task is performed daily. Click **Details** to see view detailed revocation information. Revocation requests that are not acted upon during the revocation phase can be escalated as needed.
End Period Enter Rule	Select a rule to run when the certification begins its end period.
Process Revokes Immediately	Select this option to specify that revocation requests are processed as soon as a revocation decision is saved. If this field is not selected, revocation requests are not sent until the certification is signed off. If the challenge period is active, the revocation request is not sent until the revocation is accepted or the challenge period expires.
Enable Automatic closing	Select this option to automatically close the review after the specified parameters are met. This option closes unfinished reviews.
Notifications: **These options specify when reminders and escalations occur for certification and revocations.**	
Suppress Initial Notifications	Prevent the sending of an initial notification.
Initial Notifications Email Template	Set the default email template for initial certification notifications.

Table 2—Certification Event field descriptions

Field Name	Description
Notify Before Certification Expires	Send email reminders before certification expires. Send the first reminder: The number of days before the certification expiration date that the first reminder is sent. Reminder Frequency: The frequency with which email reminders are sent until the request is completed or expires. Reminder Email Template: The IdentityIQ notification template used for the reminders.
Escalate Before Certification Expires	Send an escalation notice and change the owner of the certification to the escalation recipient. Escalation Trigger: The number of days after which a certification is assigned, or the number of email reminders that are sent to the certification owner, before the first escalation notice is sent. Escalation Rule: The escalation rule to apply when escalating a certification request.
Send Revocation Reminder	Send email reminders before the revocation period expires. Send the first reminder: The number of days before the revocation expiration date that the first reminder is sent. Reminder Frequency: The frequency with which email reminders are sent until the request is completed or expires. Reminder Email Template: The IdentityIQ notification template used for the reminders.
Escalate Revocation	Send an escalation notice and change the owner of the revocation request to the escalation recipient. Escalation Trigger: The number of days after which a revocation request is assigned, or the number of email reminders that are sent to the revocation request owner, before the first escalation notice is sent. Escalation Rule: The escalation rule to apply when escalating a revocation request.
Notify Users Of Revocations	Set the default email template for initial certification notifications.
Bulk Reassignment Modification Notices	Set the default email template for bulk reassignment notifications.
Behavior: **These advanced options specify items that can change the presentation and behavior of the certification.**	
Require Electronic Signature	Enable this option to require an electronic signature as part of the Sign-off procedure. Select the electronic signature meaning from the Electronic Signature Meaning drop-down list. An electronic signature performs the same authorization checking as the IdentityIQ login page.
Require Subordinate Completion	Enable this option to require that all subordinate access reviews be completed before the parent report can be completed.

Table 2—Certification Event field descriptions

Field Name	Description
Automatically Sign Off When Nothing to Certify	Enable this option to automatically sign off an access certification, with the assignee's credentials, if the access review contains no items, even if there are subordinate access reviews present. Access reviews containing no items and having no subordinate access reviews are always automatically signed off on using the certification initiator's credentials.
Suppress Notification When Nothing to Certify	Do not send notification email when the assignee has nothing to certify.
Require Reassignment Completion	Enable this option to require that all reassignment access reviews be completed before the parent report can be completed.
Return Reassignments to Original Access Review	Enable this option to cause the contents of reassignment access reviews to revert to the original access review when the reassigned access review is signed.
Automatically Sign Off When All Items Are Reassigned	Enable this option for an access review to be automatically signed off when all items in the access review are reassigned. **Note: The Require Reassignment Completion and Return Reassignments to Original Access Review options must not be enabled for this option to be available.**
Require Delegation Review	Enable this option to require the original access review owner to review all delegated access reviews.
Require Comments For Approval	Enable this option to require the certifier to include comments when an access review item is approved.
Require Comments When Allowing Exceptions	Enable this option to require the certifier to include comments when an exception is allowed.
Require Comments for Revocation	Require the certifier to include comments when a certification item is revoked.
Disable Delegation Forwarding	Select to disallow the forwarding of a work item that was delegated by a different user.
Limit Reassignments	Limit the number of times an item can be reassigned with a certification champaign.
Enable Line Item Delegation	Enable this option to allow certifiers to delegate individual items from an access review.
Enable Identity Delegation	Enable this option to allow certifiers to delegate entire identities in an access review.
Enable Account Revocation	Enable this option to allow users to bulk revoke all entitlements for a specific account.
Enable Allow Exceptions (applies only to non-policy violation items)	Enables certifiers to allow exceptions on access review items such as roles or entitlements, that are not policy violations. Allowing an exception means the user should not have access indefinitely, but can retain access for a specified period of time.

Table 2—Certification Event field descriptions

Field Name	Description
Deprovision Items When Exception Expires (applies only to non-policy violation items)	Enables automatic deprovisioning of access when the allowed exception period has expired. This setting applies only to items such as roles or entitlements, that are not policy violations. This option is available only when the **Enable Allow Exceptions** option is also enabled.
Enable Allow Exception Popup	Enable this option to allow certifiers to view the Allow Exception popup and manually set expiration dates and allow comments. This applies to both violation and non-violation items.
Default Duration for Exceptions	Set a default time period in which exceptions are allowed during the access review.
Enable Bulk Approval	Enable this option to allow users to bulk approve access review items.
Enable Bulk Revocation	Enable this option to allow users to bulk revoke access review items.
Enable Bulk Allow Exceptions	Enable this option to allow users to allow exceptions in bulk.
Enable Bulk Reassignment	Enable this option to allow users to bulk reassign access review items.
Enable Bulk Account Revocation	Enable this option to allow users to revoke all entitlements for a specific account in bulk. **Note: This option is not available for Entitlement Owner certifications.**
Enable Bulk Clear Decisions	Enable certifiers to cancel all decisions currently made on the access review.
Advanced: **These advanced options specify items that can change the contents and behavior of the certification.**	
Custom Name	Specify the custom name template used to name certifications. The name can contain parameterized content that is merged into the name when the certification is generated.
Custom Short Name	Specify the custom short name template used to give certifications short names. The name can contain parameterized content that is merged into the short name when the certification is generated.
Exclusion Rule	Select the rule to run to exclude specific entitlements from the certification. For example, if you have an entitlement that is assigned to every user in your enterprise, you generally do not need to include it in certifications.
Save Exclusions	Select this option to save any entitlements that are discovered, but excluded from the certification enabling them to be used in reports.
Exclude Inactive Identities	Select this option to exclude inactive identities from new certifications and remove identities that become inactive from existing certifications.
Exclude Logical Tier Entitlements	Select this option to exclude entitlements on tier application accounts from the certification. This option applies to composite applications.
Filter Logical Application Entitlements	Select this option to allow logical entitlements defined on the logical application's managed entitlement list to be included in the certification. Any logical application entitlements are filtered from the tier application entitlements

Field Name	Description
Include IdentityIQ Capabilities	Select this option to include IdentityIQ capabilities of the identity for certification.
Update Entitlement Assignments	Select this option to update assignments after entitlement decisions are made.
Pre-delegation Rule	**Note: Automated pre-delegation and pre-reassignment rules are not meant to be run in conjunction with the Fallback Forwarding User rule.** Specify the rule to use to determine if portions of the certifications that this schedule generates need be pre-delegated to specific certifiers.
Sign Off Approver Rule	Specify the rule that is used to determine if additional review is need on the sign off decision. After the certifier's initial sign off, this rule is run to determine if another approver need to review the decisions need to be reviewed. If additional review is needed, the certification request is sent to that user's inbox and they receive an email notification. This process is repeated until no more reviewers are discovered by the rule.

Chapter 11: Manage and Schedule Certifications

Note: **The term account group can be replaced by the term application object for some applications. Some application can have multiple application objects. An account group can be the name of one of those objects.**

IdentityIQ automates and optimizes the review and approval of:

- Identity access privileges
- Account group permissions and membership
- Role composition and membership

Use the Certifications page to view and create the scheduled certifications that are required to maintain compliance in your enterprise. You can also use this page to create one-time certifications when required. From this page, you can create certifications for your entire enterprise or for one approver or one item.

Certifications include multiple access reviews. When a certification schedule is created the work item arrives labeled as an access review request.

The Certification Page contains the following areas:

- "Certifications Tab" on page 59
- "Certification Events" on page 51
- "Schedule New Certification" on page 62

Certifications Tab

Use the Certifications tab to view certification requests that are complete or in the process of running.

Table 1—Certifications Tab Column Descriptions

Column	Description
Name	The type of certification scheduled and the date and time when it was first launched.
Owner	The user that started the certification request
Status	Current status of the certification request. Pending, Active, or Staged.
Percent Complete	Percentage of certification completion based on the number of access reviews in the certification.
Create Date	The date and time when the certification request was generated.
Tags	Assigned labels that are used to classify certifications for searching and reporting.

The detailed results page contains all of the information that is available for the scheduled certifications.

Click a certification to display the detailed results page for that certification. Right-click and select **Change Owner** to assign a new owner for this certification or select **Use as Template** to use this certification as a template to schedule a new certification.

> **Note:**   A change to the owner does not reassign or forward this certification to the new owner and no notification is sent to the new owner upon the change. The new owner name is associated with the certification throughout IdentityIQ.

The Certification Results page displays the name and owner of the certification, the date it was created, and status bars to track completion of the reviews, including the information described in Table 2, "Certification Results - Details Panel Descriptions," on page 60. For each access review, a description of the access review, including additional information, is described in the Access Reviews section of the table.

Table 2—Certification Results - Details Panel Descriptions

Item	Description
View Certification Options	Click to view all of the certification parameters.
Exclusions	Click to view which items were not included in the certification.
completed	The date and time when the certification request was completed. The completed status is based on the completion of all certification components.
Decision Statistics	
Roles	Pie chart with statistical data for open, approved and remediated business role items for the access reviews within the certification. **Note: This pie chart is only visible if Include Roles was enabled in the Basic section of the certification schedule creation.**
Additional Entitlements	Pie chart with statistical data for open, approved and remediated entitlement items for the access reviews within the certification. **Note: This pie chart is only visible if Include Additional Entitlements was enabled in the Basic section of the certification schedule creation.**
Policy Violations	Pie chart with statistical data for open, allowed and remediated policy violations for the access reviews within the certification. **Note: This pie chart is only visible if Include Policy Violations was enabled in the Basic section of the certification schedule creation.**
Access Reviews	
Description	The type of certification.
Percent Complete	The percentage of the certification that is complete. For example, 46% (6 of 13) means 6 of the 13 users on the list, or 46% of the total number, have been acted upon.

Table 2—Certification Results - Details Panel Descriptions

Item	Description
Phase	The current phase of the certification process. **Note: The challenge and revocation phases are only active if those functions were activated when the certification request was scheduled.** **Active** — the time period when the certifier must make all decisions required to complete the certification. **Challenge** — the time period when the affected user can challenge the decisions to revoke roles or entitlements. **Revocation** — the time period when all revocation work is expected to be completed for roles or entitlements that were revoked. Reminder notifications and escalations can be set based on these completion expectations. **End** — the certification is complete.
Phase End	The date and time when the current phase ends and the next phase begins. The length of each phase is specified when the certification request is scheduled.
Tags	Tags are used to classify certifications for searching and reporting. Tags are assigned when certifications are scheduled.
Certifiers	The name of the person responsible for acting on the access review.
Due	The date and time when the access review decision is required.
E-signed	A check-mark icon indicates that an electronic signature exists. An electronic signature performs the same authorization checking as the IdentityIQ login page.

The information displayed for each certification varies based on the type of certification and the parameters specified when the schedule is created.

For example, a manager certification results page can contain the number of access reviews that were generated, the managers who were assigned the requests, and the active period for this schedule.

Certification Schedules Tab

Use the Certification Schedules tab to view and edit information about pending and periodic.

> **Note:** Certifications that are scheduled to run one time are considered to be pending and are removed from the list of scheduled certifications after the scheduled run time.

Periodic certifications are scheduled to run on a periodic basis, such as hourly, daily, weekly, monthly, quarterly, and annually. Periodic access reviews provide a snapshot view of the identities, roles, and account groups in your enterprise. Periodic certifications focus on the frequency that entire entities (identities, roles, account groups) must be certified.

Periodic certifications are not complete until all access reviews included in the certification are complete. An access review is not complete until all actions are complete and the user who is assigned the access review confirms the decisions.

Periodic certifications can be created using a multi-level sign-off structure which enables multiple certifiers to review access reviews before they are considered complete. For example, a certification can be created for the direct reports of a team leader who knows his employees, but is not authorized to make final certification

decisions. When the team leader makes his decisions and signs off on the access review, it can be forwarded to the department manager to review the decisions and make changes if necessary.

The Certifications Schedule tab contains the following information:

Table 3—Certifications Schedule Tab Column Descriptions

Column	Description
Name	The type of certification scheduled and the date and time when it was launched.
Task	The task that was performed.
Next Execution	The next date and time when the certification runs.
Last Execution	The date and time when the certification ran last.
Result	Result status of the last run of the certification, for example Success or Failed.
Owner	The user who started the certification request

Click an existing certification to view the details defined for the certification when it was created. Certifications can be modified for future certifications. Actions that were taken on the access reviews included in the certification and the current phase of the certification determine which items can be modified.

Schedule New Certification

Note: **Identity certifications are special cases and are scheduled from the Identities or Advanced Identity Search Results pages. Any IdentityIQ user with access to those pages can schedule an identity certification.**

Use the **Schedule New Certification** drop-down list to schedule certifications.

You can also schedule a certification by right-clicking an existing certification and selecting **Use Certification as a Template**.

Note: **Identity Certifications are not scheduled from the Certifications page, they are requested from the Identity Risk Scores, Identity Search Results or Policy Violations pages.**

Note: **Automatic approvals are not dismissed in the access reviews if you turn off the automatic approval feature and then activate a staged certification. To remove automatic approvals access reviews generated by a staged certification, you must delete and redefine the certification.**

To generate a preview of a certification, enable the staging feature on the Lifecycle panel on the Schedule Certification page for non-targeted certifications or on the Schedule panel for targeted certifications. When the staging feature is enabled, a certification and associated access reviews are created, but the access reviews are not sent to the certifiers. You can view what the certification schedule definition produces before the schedule is activated. If the generated certification does not match your needs, you can cancel the certification and redefine it as needed. If the certification is accurate, activate the schedule.

"Schedule Non-Targeted Certification Field Descriptions" on page 63

"Schedule Targeted Certification Field Descriptions" on page 29

Schedule Non-Targeted Certification Field Descriptions

This section describes all fields included in any non-targeted certification schedule. Fields or options that are available for a specific type of certification are listed in a separate column.

Basic Fields

The Basic page includes general information about the certification including the name, owner, and various controls about when and how often to run it. This page also includes a number of fields that are specific to a limited set of certification types.

Note: **Certification start times must be at least one minute later than the current time. For example, if it is currently 11:41, the certification start time must be 11:42 or later.**

Note: **Certifications that run across time zones run at the time scheduled, relative to the time zone in which they are scheduled. For example, a certification scheduled to run at 1:00 PDT will run at 4:00 EDT.**

Table 4—Basic Field Descriptions

Field Name	Certification Type	Description
Certification Name	All	Specify a name and date parameter that identifies the certification.
Certification Owner	All	Specify an owner of the certification.
Recipient	Manager	The full name of a specific manager being assigned a certification. To display a list of all of the manager names in the system, type the first few letters of the name. You can select a name from the displayed list.
All Managers	Manager	Schedule a certification for all managers configured in the IdentityIQ application.
Application(s)	Application Owner Entitlement Owner Account Group	Select the applications to certify. Use the Ctrl or Shift keys to select multiple applications or select **All Applications**.
All Applications	Application Owner Entitlement Owner Account Group	Include all applications in the certification.

Table 4—Basic Field Descriptions

Field Name	Certification Type	Description
Populations to Certify	Advanced	**Population** — All available populations IdentityIQ. Includes all public populations and populations you created.
		Certifier(s) — The identities who are requested to complete the certification request. Certifiers can be individual identities or workgroups. To display a list of all of the manager names in the system, type the first few letters of the name. You can select a name from the displayed list. **Note: A separate certification request is sent for each population specified, even if the certifier of each is the same.**
Group Factories to Certify	Advanced	**Group Factory** — All available groups created by group factories and includes all identity attributes designated as group factories.
		Certifier Rule — Select the rule used to designate certifiers for the groups selected.
Certifiers	Identity	Select the person or people to review the certification. Options include assigning managers or manually selecting certifiers.
Identities	Identity	Lists each identity included in the certification. To remove identities, select an identity and click **Remove Selected Users**. To add identities type a name in the field and click **Add User**.
Included Applications	Manager Identity	The applications included when generating this certification. If no applications are specified, all of the applications are included.
Select Role(s)	Role Membership Role Composition	To specify roles to certify, select a role from the list. To specify a role type to certify, click the **Certify by Role Type** radio button and select the role type from the list. **Note: When you include business roles, all assigned business roles are displayed in the certification.**
Certify All Roles	Role Membership Role Composition	Schedule a certification on all roles defined in your enterprise.
Include Role Hierarchy	Role Composition	Create certification items for each role that is included in the roles selected for certification.

Table 4—Basic Field Descriptions

Field Name	Certification Type	Description
Included Access	Manager Application Owner Identity	Select Entitlements to include entitlement access in the certification. You can also choose to include Additional Entitlements, Roles and Accounts With No Entitlements in the certification. You must select Accounts to include from accounts in the certification. **Note: The Include Roles option is enabled by default and all assigned business roles are displayed in the certification.**
Include Policy Violations	All	Include policy violations for each identity in the certification report.
Include Unowned Data	Entitlement Owner	Select this option to include managed entitlements and permissions that have no owner in the access review.
Unowned Entitlement Reviewer	Entitlement Owner	Select this option to assign ownership of unowned entitlements to the application owner or an identity you select from the drop-down list.

Lifecycle Fields

Fields in the Lifecycle page enable you to define various time periods in the certification process.

Table 5—Lifecycle Field Descriptions

Field Name	Description
Enable Staging Period	Use to generate a test certification that is used to verify functionality and configuration of the parameters before the certification is generated. The test certification displays in the Certifications tab with the status set to Staged. Click the certification to view it is contents and either activate or cancel it. **Note: You might experience a short delay between scheduling the test certification and seeing it on the Certifications tab with all of the data displayed.** **Note: Automatic approvals are not dismissed in the access reviews if you turn off the automatic approval feature and then activate a staged certification. To remove automatic approvals access reviews generated by a staged certification, you must delete and redefine the certification.**
Active Period Enter Rule	Select a rule from the drop-down list to apply when the certification enters its active period.

Table 5—Lifecycle Field Descriptions

Field Name	Description
Active Period Duration	Specify the review period when all decisions required within this certification must be made. During this phase changes can be made to decisions as often as needed. You can sign off on a certification in the active period only if no roles or entitlements were revoked or if the challenge period is not active. When you sign off on a certification, the certification enters the end phase or the revocation phase. To enter the revocation phase, the revocation period must be active and a revocation decision must exist.
Enable Challenge Period	Specify the period when all revocation requests can be challenged by the user from which the role or entitlement is being removed. When the challenge phase begins, a work item and email are sent to each user in the certification that the revocation decision affects. The work items include the details of the revocation request and any comments the requestor added. The affected user has the duration of the challenge period to accept the loss of access or challenge that decision. You can sign off on a certification in the challenge phase if all challenges were completed and no open decisions remain on the certification. When you sign off on a certification, it enters the end phase or the revocation phase. To enter the revocation phase, the revocation period must be active and a revocation decision must exist. **Note: This option is not available for Role Composition and Role Membership certifications.**
Challenge Period Enter Rule	Select a rule from the drop-down list to apply when the certification enters its challenge period.
Challenge Period Duration	Specify the period of time when items remain in the challenge period.
Challenge Email Templates	Choose the email templates used for a variety of challenge period notifications.
Enable Revocation Period	**Note: If the revocation period is disabled, the certification is not scanned for completed revocations and revocation status might not be accurately reflected throughout the product.** Specify the period when all revocation work must be completed. When the revocation phase is entered, revocation is done automatically if your provisioning provider is configured for automatic revocation or manually using a work request assigned to an IdentityIQ user with the proper authority on the specified application. The revocation phase is entered when a certification is signed off or when the active and challenge phases have ended. Revocation activity is monitored to ensure that inappropriate access to roles and entitlements is revoked in a timely manner. Revocation completion status is updated at an interval specified during the deployment of IdentityIQ. By default this is performed daily. Click **Details** to view detailed revocation information. Revocation requests that are not acted upon during the revocation phase can be escalated as required.

Table 5—Lifecycle Field Descriptions

Field Name	Description
Revocation Period Enter Rule	Select a rule from the drop-down list to apply when the certification enters its revocation period.
Revocation Period Duration	The period of time when items remain in the revocation period.
End Period Enter Rule	Select rule to run when the certification enters the end period.
Process Revokes Immediately	Specifies that revocation requests must be processed as soon as a revocation decision is saved. If this field is not activated, revocation requests are not sent until the certification is signed off. If the challenge period is active, the revocation request is not sent until the revocation is accepted or the challenge period expires.
Enable Automatic Closing	Specifies that decisions not made by the certifier during the active phase are made automatically. Use the following options to configure the details of this process. **Time After Certification Expiration** - Select the amount of time following this access review's expiration date that IdentityIQ must wait before attempting to automatically close it. **Closing Rule** - Select the rule that IdentityIQ runs at the beginning of the automatic closing process. **Action Taken On Undecided Items** - The action that IdentityIQ assigns to any undecided items when automatically closing this access review. Choose from Approve, Revoke, or Allow Exception. **Comments** - Input the comments that IdentityIQ adds to any undecided items when automatically closing this access review.

Notifications Field Descriptions

Fields in the Notifications page enables you to configure when reminders and escalations must occur for both certifications and revocations.

> **Note:** Some of these options are not available on Identity, Application Owner, and Advanced certifications.

Table 6—Notifications Field Descriptions

Field Name	Description
Suppress Initial Notifications	Select this option to prevent the sending of initial certification notification emails.
Initial Notification Email Template	Choose the email template used for initial certification notifications.
Notify Before Certification Expires	Send email reminders before certification expires.

Field Name	Description
Send Revocation Reminders	Send email reminders before the revocation period expires. Includes when the first reminder is sent, how often reminders are sent, and which template to use for the reminders.
Escalate Revocations	Send an escalation notice and change the owner of the revocation request to the escalation recipient. Includes settings for: • Number of reminders to send to the revocation request owner before the first escalation occurs • Escalation rule to apply when escalating an uncompleted revocation request • Email template to use for the escalation notice
Notify Users Of Revocations	Send an email notification to identities whose access was revoked. **Note: This option is not available for Account Group Permissions or Role Composition certifications.**
Bulk Reassignment Modification Notices	Choose the email template to use to send bulk reassignment notices

Behavior Fields

Fields in the Behavior page enables you to change the presentation and behavior of the certification.

Field Name	Description
Prompt for Signoff	Enable this option to display a pop-up reminder to indicate when an access review is complete and ready for sign-off.
Require Electronic Signature	Enable this option to require an electronic signature as part of the Sign-off procedure. Select the electronic signature meaning from the Electronic Signature Meaning drop-down list. An electronic signature performs the same authorization checking as the IdentityIQ login page.
Require Subordinate Completion	Enable this option to require that all subordinate access reviews be completed before the parent report can be completed.
Automatically Sign Off When Nothing to Certify	Enable this option to automatically Sign Off an access certification, with the assignee's credentials, if the access review contains no items, even if there are subordinate access reviews present. Access reviews containing no items and having no subordinate access reviews are always automatically signed off using the certification initiator's credentials.
Suppress Notification When Nothing to Certify	Do not send notification email when the assignee has nothing to certify.
Require Reassignment Completion	Enable this option to require that all reassignment access reviews be completed before the parent report can be completed.

Table 7—Behavior Field Descriptions

Field Name	Description
Return Reassignments to Original Access Review	Enable this option to cause the contents of reassignment access reviews to revert to the original access review when the reassigned access review is signed.
Automatically Sign Off When All Items Are Reassigned	Enable this option for an access review to be automatically signed off when all items in the access review are reassigned. **Note: The Require Reassignment Completion and Return Reassignments to Original Access Review options must not be enabled for this option to be available.**
Require Delegation Review	Enable this option to require the original access review owner to review all delegated access reviews.
Require Comments For Approval	Enable this option to require the certifier to include comments when an access review item is approved.
Require Comments When Allowing Exceptions	Enable this option to require the certifier to include comments when an exception is allowed.
Require Comments for Revocation	Require the certifier to include comments when a certification item is revoked.
Disable Delegation Forwarding	Select to disallow the forwarding of a work item that was delegated by a different user.
Limit Reassignments	Enable this option to allow users to limit the number of reassignment of certification item.
Show Classifications	Show classification information in identity-based access reviews. When enabled, classifications provide additional information about roles, managed attributes and policy violations. Note that this option is available only in identity-based certifications.
Enable Line Item Delegation	Enable this option to allow certifiers to delegate individual items from an access review.
Enable Identity Delegation	Enable this option to allow certifiers to delegate entire identities in an access review.
Enable Account Revocation	Enable this option to allow users to bulk revoke all entitlements for a specific account.
Enable Allow Exceptions (applies only to non-policy violation items)	Enables certifiers to allow exceptions on access review items such as roles or entitlements, that are not policy violations. Allowing an exception means the user should not have access indefinitely, but can retain access for a specified period of time.
Deprovision Items When Exception Expires (applies only to non-policy violation items)	Enables automatic deprovisioning of access when the allowed exception period has expired. This setting applies only to items such as roles or entitlements, that are not policy violations. This option is available only when the **Enable Allow Exceptions** option is also enabled.
Enable Allow Exception Popup	Enable this option to allow certifiers to view the Allow Exception popup and manually set expiration dates and allow comments. This applies to both violation and non-violation items.

Field Name	Description
Default Duration for Exceptions	Set a default time period in which exceptions are allowed during the access review.
Show Recommendations	**Note: This option is only visible if you have purchased and activated the SailPoint IdentityAI product** **Note: This feature is only available on Manager, Application Owner, Advanced, and Role Membership certifications.** Enable recommendations from IdentityAI to display in access reviews.
Automatically Approve Recommended Items	**Note: This option is only visible if you have purchased and activated the SailPoint IdentityAI product** **Note: This feature is only available on Manager, Application Owner, Advanced, and Role Membership certifications.** Automatically mark access review items as approved and move them from the Open to the Review tab of the access review.
Enable Bulk Approval	Enable this option to allow users to bulk approve access review items.
Enable Bulk Revocation	Enable this option to allow users to bulk revoke access review items.
Enable Bulk Allow Exceptions	Enable this option to allow users to allow exceptions in bulk.
Enable Bulk Reassignment	Enable this option to allow users to bulk reassign access review items.
Enable Bulk Account Revocation	Enable this option to allow users to revoke all entitlements for a specific account in bulk. **Note: This option is not available for Entitlement Owner certifications.**
Enable Bulk Clear Decisions	Enable certifiers to cancel all decisions currently made on the access review.

Advanced Fields

Fields in the Advanced page enables you to define a variety of additional options for the certification.

Field Name	Certification Type	Description
Custom Name	All	The custom name used to name certifications. You can combine free text and parameterized text by selecting parameters from the drop-down list on the right.
Custom Short Name	All	You can combine free text and parameterized text by selecting parameters from the drop-down list on the right.

Table 8—Advanced Field Descriptions

Field Name	Certification Type	Description
Certifiers	Role Membership Role Composition	**Assign to Manager (Role Membership Only)—** assign the certification request to the role member's manager. If the role members do not share a common manager, a separate certification request will be created for each manager with at least one direct report in the role under certification. If a manager is not found for an identity, the certification is assigned to the role owner for that identity. **Assign to Role Owner —** assign the certification to the owner of the role under certification. If multiple roles have been selected, separate certifications will be created if the given roles do not share a common owner. If no role owner is discovered, a warning is attached to the task results with a list of the items that could not be assigned for certification. **Select Certifier Manually —** enter the full name of a specific certifier or certifiers being assigned this certification. Certifiers can be individual identities or workgroups. A name entered here overrides the default certifier for the type of certification requested. Typing the first few letters of the name displays a list of all of the authorized certifier names in the system containing that letter combination. You can select from the displayed list.
Certifiers	Application Owner Account Group Membership Account Group Permissions	The full name of a specific certifier or certifiers being assigned to this certification. A name entered here overrides the account group owner as certifier for this certification request. Certifiers can be individual identities or workgroups.
Generate Certifications	Manager Identity	Select whether to generate a certification request for the specified managers, or for the specified managers and all of their subordinate managers. If you select **For the specified manager(s) only**, the **Flatten Hierarchy** option is displayed. Select the **Flatten Hierarchy** option to include everyone below the manager in the reporting hierarchy on the certification request.
Exclusion Rule	All	Select the rule that should be run to exclude certain entitlements from the certification. For example, if you have an entitlement that is assigned to every user in your enterprise, you probably do not need to include it in certifications.

Table 8—Advanced Field Descriptions

Field Name	Certification Type	Description
Save Exclusions	All	Activate to save any entitlements that are discovered, but excluded from the certification so that they can be used in reports.
Exclude Inactive Identities	All except Role Composition, Account Group Permissions, and Entitlement Owner	Exclude inactive identities from new certifications and remove identities that become inactive from existing certifications.
Filter Logical Application Entitlements	All except Entitlement Owner	Only logical entitlements defined on the logical application's managed entitlement list will be included in the certification. Additionally any logical application entitlements will be filtered from the tier application entitlements.
Include IdentityIQ Capabilities	All except Entitlement Owner	Include IdentityIQ capabilities of the identity for certification.
Update Entitlement Assignments	All except Entitlement Owner	Enable to have decisions made on entitlement values in the access review apply to the entitlement assignment model. When enabled, approvals create assignments and revocations remove assignments.
Pre-delegation Rule	All	Specify the rule to use to determine if portions of the certifications generated by this schedule should be pre-delegated or reassigned to specific certifiers.
Sign Off Approver Rule	All except Role Composition	The rule used to determine if additional review is needed on the Sign Off decision. After the initial Sign Off by the certifier, this rule is run to determine if the decisions need to be reviewed by another approver. If they do, the certification request is sent to that user's inbox and they receive an email notification. This process is repeated until no more reviewers are discovered by the rule. You must also select the email template used for Sign Off approvers.
Allow Self Certification For	All except Role Composition and Account Group Permissions	Choose which users may self-certify (that is, be the certifier for their own access), either by forwarding or reassigning an access review: All certifiers, Certification and System Administrators, System Administrators only

Table 8—Advanced Field Descriptions

Field Name	Certification Type	Description
Self Certification Violation Owner	All except Role Composition and Account Group Permissions	For users that are not allowed to self-certify, this is the identity or workgroup that will receive any items that would require a self-certification - that is, when the reviewer and the user whose access is under review are the same person. If a Self Certification Violation Owner is not specified, any items that require self-certification will be read-only to the reviewer.
Enable Partitioning	Manager	Enable the use of multiple threads to schedule the certification

Schedule Targeted Certification Field Descriptions

This section describes all fields included in a targeted certification schedule.

Who to Certify

To narrow down the identities to certify, choose an option for selecting identities. To certify all identities in your system, do not define any selection criteria.

Table 9— Targeted Certification - Who To Certify

Field Name	Description
Filter	Use filters to define the identity list the certification. You can choose the values for the filter from a list, or type them in. You can only type in valid values. - Select Attribute — a list of every searchable attribute defined in IdentityIQ - Operator — a list of valid operators, such as Equals or Starts With, for the selected attribute - Text field or drop-down list, depending on the operator selected departments will select identities from both those departments. You can choose more than one value for any one filter. When you do this, the criteria works as an "or" operation, so the certification will include all identities meeting any of the criteria. For example, filtering on Department Equals and entering two departments will select identities from both those departments. Use **Add Filter** to define as many filters as needed. When you add multiple filters, identities have to meet each of the sets of filter criteria in order to be included. For example, filtering on Department Equals Accounting and Location Equals Berlin will select only identities that are in the Accounting department in Berlin **Note: Access reviews for Service or RPA/Bot identities are sent to the certifier specified during your configuration process.**

Field Name	Description
Population	Enter the name of an existing population or select one from the drop-down list. Populations are saved queries based on searches run from the Identity Search feature of Advanced Analytics
Rule	**Note: This must be an identity inclusion rule for Targeted certifications.** Choose a rule that will select identities. The Targeted Certification does not include a rule editor, so you are limited to choosing existing rules from the list. Only rules with a rule type of CertificationScheduleEntitySelector are included in this list.
Exclude Inactive Identities	Check this to omit identities flagged as Inactive at the time the certification is generated. For recurring certifications, future occurrences will reflect any changes that have happened since the last certification was generated, including identities that have become inactive.

What to Certify

This section lets you narrow the focus of the certification by defining which elements of accounts, roles, entitlements, and target permissions to include.

Role/Entitlements/Target Permissions

Use the **Roles**, **Additional Entitlements**, and **Target Permissions** options to include roles, additional entitlements, and target permissions in the certification. Target Permissions are the actions a user can perform on an unstructured target such as a file share or folder.

Use **Filter Roles**, **Filter Entitlements**, and **Filter Target Permissions** to set your criteria for choosing what to certify. You can choose more than one value for any one filter. When you do this, the criteria works as an "or" operation, so the certification will include all entities meeting any of the criteria. For example, filtering on Owner Equals and entering two identities will select roles/accounts owned by either of those identities.

Use **+Add Filter** to include multiple filters for roles and entitlements. This lets you filter on more than one attribute using an "and" condition. With multiple filters, entities have to meet each of the sets of filter criteria in

order to be included. For example, filtering accounts on Service Account Equals True and Application Equals Active_Directory will select only service accounts on the Active Directory application

The filters types supported in roles/entitlements are:

- Boolean:
    - **Operators**: None
    - **Values**: True, False
- Date:
    - **Operators**: before, after, between, equals, not equals
    - **Values**: Date Picker
- Identity:
    - **Operators**: None
    - **Values**: Identity Picker
- Integer:
    - **Operators**: is, is not, greater than, less than
    - **Values**: dropdown with prefilled values
- Rule:
    - **Operators**: None
    - **Values**: Rule picker
- String:
    - **Operators**: is, is not, starts with
    - **Values**: text field

Table 10— Targeted Certification - What to Certify - Roles\Entitlements

Field Name	Description
Certifying All ...	Include all IdentityIQ roles or additional entitlements
Filter Roles	Define filters to limit the roles included in the certification
Select Attribute	Select a role\entitlement attribute from the drop-down list
Operator	Select an operator from the drop-down list for this attribute
Value	Select a value from the drop-down list The values available are dependent on the attribute and operator selected
Include Accounts without Entitlements	Include accounts that have no entitlement attributes.

Target Permissions

Use **+Add Filter** to include multiple filters for target permissions.

The filters types supported in target permissions are:

- Boolean:

    - **Operators**: None

    - **Values**: True, False

- Date:

    - **Operators**: before, after, between, equals, not equals

    - **Values**: Date Picker

- String:

    - **Operators**: is, is not, starts with

    - **Values**: text field

Table 11— Targeted Certification - What to Certify - Target Permissions

Field Name	Description
Certifying All Target Permissions	Include all Include IdentityIQ target permissions
Filter Target Permissions	Define filters to limit the target permissions included
Select Attribute	Select an target permission attribute from the drop-down list
Operator	Select an operator from the drop-down list for this attribute
Value	Select a value from the drop-down list The values available are dependent on the attribute and operator selected

Accounts Only

Use **+Add Filter** to include multiple filters for accounts.

The filters types supported in accounts are:

- Boolean:
  - **Operators**: None
  - **Values**: True, False
- Date:
  - **Operators**: before, after, between, equals, not equals
  - **Values**: Date Picker
- String:
  - **Operators**: is, is not, starts with
  - **Values**: text field

Table 12— Targeted Certification - What to Certify - Accounts Only

Field Name	Description
Certifying All Accounts	Include all Include IdentityIQ accounts
Filter Accounts	Define filters to limit the number of accounts included
Select Attribute	Select an account attribute from the drop-down list
Operator	Select an operator from the drop-down list for this attribute
Value	Select a value from the drop-down list The values available are dependent on the attribute and operator selected

Shared Options

Table 13— Targeted Certification - What to Certify - Shared Options

Field Name	Description
Include Policy Violations	Policies are rules that enforce your enterprise's business policies on separation of duty, activity, and risk. Violations of those policies can be included in the access reviews generated by the certification.
Exclude Logical Tier Entitlements	Logical applications are applications formed by the detection of accounts from other applications, called "tier" applications, in existing Identity Cubes. Use this option to exclude entitlements on tier application accounts from the certification. This applies only to logical applications.
Filter Logical Application Entitlements	Allow logical entitlements defined on the logical application's managed entitlement list to be included in the certification. Any logical application entitlements are filtered from the tier application entitlements.
Include IdentityIQ Capabilities	Capabilities control access to pages, tabs, and fields within IdentityIQ. Use this option to include IdentityIQ capabilities in the certification.

Table 13— Targeted Certification - What to Certify - Shared Options

Field Name	Description
Include IdentityIQ Scopes	Scopes are used to restrict access to objects in IdentityIQ. If scoping is enabled in your implementation, use this option to include scopes in the certification

Choose Certifier

Select a recipient for this certification.

Targeted certifications are designed to enable you to get very specific on the certification scheduling page to select exactly who should be the certifier for the certification.

Tools are provide that should eliminate the need to reassign certifications. This design provides the flexibility of rules from the user interface so that you can schedule certifications without having to write rules.

If required, reassignment can be performed by specifying a Certifier type rule in the Primary Certifier field.

For example, if the certifier should be a manager except if the target identity is a manager herself or has no manager, a Certifier type rule can contain the following:

```
import sailpoint.object.Identity;

    Identity target = entity.getIdentity(context);

    if (target.getManagerStatus() || (target.getManager() == null)) {

        return "spadmin";

    }

    return target.getManager().getName();
```

Pre-delegation rules can still be used to support the Delegation and Forwarding of access reviews, but any reassignment components are ignored.

Table 14— Targeted Certification - Choose Certifier

Field Name	Description
Primary Certifier	**Manager** - the manager of each identity included in the certification. **Owner** - roles are certified by the role owner, accounts by the application owner, additional entitlements by the application or entitlement owner. **Note: Pre-delegation rules do not support reassignments in the Targeted Certification. Use the Primary Certification field in a Certifier type rule for reassignment** **Rule** - choose the certifier using a rule. The Targeted Certification does not include a rule editor, so you are limited to choosing an existing rules from the list. Only rules with a rule type of Certifier are included in this list. A backup certifier is also required. You can also use a Certifier Rule to control reassignments. **Single Certifier** - select a certifier from the drop-down list
Backup Certifier	A backup certifier is required for all types of Primary Certifier except single certifier
Advanced Options:	
Reassignments	

Table 14— Targeted Certification - Choose Certifier

Field Name	Description
Enable Bulk Reassignment	Allow reviewers to reassign multiple items simultaneously within an access review.
Limit Reassignments	Limit the number of times reviewers can reassign an item in the access review. If you opt to limit reassignments, include the number of reassignments allowed.
Require Reassignment Completion	Require that all reassignment access reviews be completed before the parent report can be completed.
Return Reassignments to Original Access Review	When a reassigned review is signed off, return the reassigned review to the original access review owner. When items are returned, the original owner can modify the decisions the reassigned reviewer has made.
Automatically Sign Off When All Items Are Reassigned	Allow the access review to be automatically signed off when all items in the access review are reassigned. **Note: This option can only be enabled if the Require Reassignment Completion and Return Reassignments to Original Access Review options are NOT enabled.**
Bulk Reassignment Modification Notices	Choose the email template to use to send bulk reassignment notices
Self Certification	
Allow Self Certification For	Choose which users may self-certify - that is, be the certifier for their own access, either by forwarding or reassigning an access review: All certifiers, Certification and System Administrators, System Administrators only
Self Certification Violation Owner	For users that are not allowed to self-certify, this is the identity or workgroup that will receive any items that would require a self-certification - that is, when the reviewer and the user whose access is under review are the same person. If a Self Certification Violation Owner is not specified, any items that require self-certification will be read-only to the reviewer.
Other	
Prompt for Sign Off	Display an overlay prompting reviewers to sign off, when the access review is complete.
Require Electronic Signature	Require an electronic signature as part of the Sign-off procedure. Reviewers use their IdentityIQ login credentials as authorization for the electronic signature. If you opt to require electronic signature, select the Electronic Signature Meaning; this is the text that goes with the electronic signature, and is defined in Global Settings > Electronic Signatures.
Automatically Sign Off When Nothing to Certify	Enable this option to automatically sign off an access certification, with the assignee's credentials, if the access review contains no items, even if there are subordinate access reviews present Access reviews containing no items and having no subordinate access reviews are always automatically signed off on using the certification initiator's credentials

Field Name	Description
Suppress Notification When Nothing to Certify	Do not send notification email when the assignee has nothing to certify
Sign Off Approval Rule	A rule used to determine if additional review is need on the sign off decision. After the initial sign off by the certifier, this rule is run to determine if the decisions need to be reviewed by another approver. If they do, the certification request is sent to that user's inbox and they receive an email notification. This process is repeated until no more reviewers are discovered by the rule. You must also select the email template used for sign off approvers
Sign Off Approval Notice Email Template	Select the email template sent if the sign off approval rule determines one is needed

Schedule

Start

> **Note:** **Certification start times must be at least one minute later than the current time. For example, if it is currently 11:41, the certification start time must be 11:42 or later.**

> **Note:** **Certifications that run across time zones run at the time scheduled, relative to the time zone in which they are scheduled. For example, a certification scheduled to run at 1:00 PDT will run at 4:00 EDT.**

> **Note:** **Automatic approvals are not dismissed in the access reviews if you turn off the automatic approval feature and then activate a staged certification. To remove automatic approvals access reviews generated by a staged certification, you must delete and redefine the certification.**

Use the staging feature to create a certification and associated access reviews, but not send the access reviews to the certifiers. You can view what the certification schedule definition produces before the schedule is activated. If the generated certification does not match your needs, you can cancel the certification and redefine it as needed. If the certification is accurate, activate the schedule.

Select an Initial Notification Email Template from the drop-down list, or **Suppress Initial Notification** to not send an email.

Active

Field Name	Description
Active Period Duration	Specify the review period when all decisions required within this certification must be made. During this phase changes can be made to decisions as often as needed. You can sign off a certification in the active period only if no roles or entitlements were revoked or if the challenge period is not active. When you sign off a certification, the certification enters the end phase or the revocation phase. To enter the revocation phase, the revocation period must be active and a revocation decision must exist.
Active Period Enter Rule	A rule to run when the certification enters its active period. Rules of type "CertificationPhaseChange" are included in the list.

Table 15— Targeted Certification - Schedule - Active

Field Name	Description
Add	Add a new reminder or escalation. Specify reminder or escalation in the drop-down list.

End

Table 16— Targeted Certification - Schedule - End

Field	Description
Enable Revocation Period:	Enabling a revocation period makes IdentityIQ periodically scan identities to determine whether the requested remediations have been carried out. Remediation occurs whether or not a Revocation period is enabled, but when the Revocation period is enabled, IdentityIQ monitors the status of remediation requests; when it is not enabled, remediation requests are processed but are not tracked. Specify the period when all revocation work must be completed. When the revocation phase is entered, revocation is done automatically if your provisioning provider is configured for automatic revocation or manually using a work request assigned to an IdentityIQ user with the proper authority on the specified application. The revocation phase is entered when a certification is signed off or when the active and challenge phases have ended. Revocation completion status is updated at an interval specified during the deployment of IdentityIQ. By default this is performed daily. Click **Details** to view detailed revocation information. Revocation requests that are not acted upon during the revocation phase can be escalated as required. **Note: If the revocation period is disabled, the certification is not scanned for completed revocations and revocation status might not be accurately reflected throughout the product.**
Revocation Period Duration	The length of the revocation period.
Revocation Period Enter Rule	A rule to run when the certification enters the revocation period. Rules of type "CertificationPhaseChange" are included in this list.
Process Revokes Immediately	Specifies that revocation requests must be processed as soon as a revocation decision is saved. If this field is not activated, revocation requests are not sent until the certification is signed off. If the challenge period is active, the revocation request is not sent until the revocation is accepted or the challenge period expires.
Revocation Notifications	Send email reminders before the revocation period expires. Includes when the first reminder is sent, how often reminders are sent, which template to use for the reminders, and who should receive them.

Table 16— Targeted Certification - Schedule - End

Field	Description
Enable Challenge Period:	A challenge period allows users to be notified of revocation decisions affecting their access. When the challenge phase begins, a work item and email are sent to each user in the certification that the revocation decision affects. The work items include the details of the revocation request and any comments the requestor added. The affected user has the duration of the challenge period to accept the loss of access, or to challenge the decision with a justification for continued access. The Challenge period begins when the Active Period ends. The certifier can consider a challenger's justification and can change decisions based on the challenge. You can sign off on a certification in the challenge phase if all challenges were completed and no open decisions remain on the certification. When you sign off on a certification, it enters the end phase or the revocation phase. To enter the revocation phase, the revocation period must be active and a revocation decision must exist.
Challenge Period Duration	The length of the challenge period.
Challenge Period Enter Rule	A rule to run when the certification enters its challenge period. Rules of type "CertificationPhaseChange" are included in this list.
Email Notifications	Choose the email templates used for a variety of challenge period notifications.
Enable Automatic Closing:	Specifies that decisions not made by the certifier during the active phase, are made automatically. Use the following options to configure the details of this process. **Time After Certification Expiration** - The amount of time following this access review's expiration date that IdentityIQ must wait before attempting to automatically close it. **Closing Rule** - The rule that IdentityIQ runs at the beginning of the automatic closing process. **Action Taken On Undecided Items** - The action that IdentityIQ assigns to any undecided items when automatically closing this access review. Choose from Approve, Revoke, or Allow Exception. **Automatic Closing Signer** - The identity or workgroup that is listed as the signer. **Comments** - Input the comments that IdentityIQ adds to any undecided items when automatically closing this access review.

Additional Settings

Table 17— Targeted Certification - Additional Settings

Field Name	Description
Certification Name	A name and date parameter to identify the certification.

Table 17— Targeted Certification - Additional Settings

Field Name	Description
Certification Owner	The identity or workgroup responsible for the certification.
Advanced Options:	
Enable Bulk Clear Decisions	Enable certifiers to cancel multiple decisions simultaneously on the access review.
Update Entitlement Assignments	Enable this option to have decisions made on entitlement values in the access review apply to the entitlement assignment model. When this is enabled, approvals create assignments and revocations remove assignments.
Enable Partitioning	Partitioning subdivides activity across multiple threads. Specify a number of partitions. If no number is specified, IdentityIQ calculates an optimal number.
Show Recommendations	**Note: This option is only visible if you have purchased and activated the SailPoint IdentityAI product.** Enable recommendations from IdentityAI to display in access reviews.
Automatically Approve Recommended Items	**Note: This option is only visible if you have purchased and activated the SailPoint IdentityAI product** Automatically mark access review items as approved and move them from the Open to the Review tab of the access review.
Show Classifications	Show classification information in the access reviews. When enabled, classifications provide additional information about roles, managed attributes and policy violations.
Delegation Options:	
Require Delegation Review	Enable this option to require the original access review owner to review all delegated access reviews.
Line Item Delegation	Enable this option to allow certifiers to delegate individual items from an access review.
Identity Delegation	Enable this option to allow certifiers to delegate entire identities in an access review.
Disable Delegation Forwarding	Select to disallow the forwarding of a work item that was delegated by a different user.
Pre-Delegation Rule	**Note: Pre-delegation rules do not support reassignments in the Targeted Certification. Use the Primary Certification field in a Certifier type rule for reassignment** Select a pre-delegation rule from the drop-down list
Email Owner on Pre-Delegation Completion	Send a email to the owner of the original certification upon completion of the certification by the delegates
Approve Options:	

Table 17— Targeted Certification - Additional Settings

Field Name	Description
Require Comments For Approval	Enable this option to require the certifier to include comments when an access review item is approved.
Enable Bulk Approval	Enable this option to allow users to bulk approve access review items.
Revoke Options:	
Enable Bulk Revocation	Enable this option to allow users to bulk revoke access review items.
Enable Account Revocation	Enable this option to allow users to bulk revoke all entitlements for a specific account.
Enable Bulk Account Revocation	Enable this option to allow users to revoke all entitlements for a specific account in bulk.
Require Comments for Revocation	Require the certifier to include comments when a certification item is revoked.
Allow Options:	
Enable Allow Exceptions (applies only to non-policy violation items)	Enables certifiers to allow exceptions on access review items such as roles or entitlements, that are not policy violations. Allowing an exception means the user should not have access indefinitely, but can retain access for a specified period of time.
Deprovision Items When Exception Expires (applies only to non-policy violation items)	Enables automatic deprovisioning of access when the allowed exception period has expired. This setting applies only to items such as roles or entitlements, that are not policy violations. This option is available only when the **Enable Allow Exceptions** option is also enabled.
Enable Bulk Allow Exceptions	Enable this option to allow users to allow exceptions in bulk.
Enable Allow Exception Popup	Enable this option to allow certifiers to view the Allow Exception popup and manually set expiration dates and allow comments. This applies to both violation and non-violation items.
Require Comments When Allowing Exceptions	Enable this option to require the certifier to include comments when an exception is allowed.
Default Duration for Exceptions	Set a default time period for which exceptions are allowed during the access review.
Access Review Properties:	
Custom Name	The custom name template used to name certifications. You can combine free text and parameterized text by selecting parameters from the drop-down list on the right.

Table 17— Targeted Certification - Additional Settings

Field Name	Description
Custom Short Name	The custom short name template used to give certifications short names displayed. You can combine free text and parameterized text by selecting parameters from the drop-down list on the right.
Tags	Labels that are used to classify certifications for searching and reporting.

Section II Configure IdentityIQ

You must setup IdentityIQ to work within your enterprise before it can help you make more strategic decisions using systems that collect, store, access and analyze corporate data from sources all across the enterprise.

Refer to your SailPoint IdentityIQ *Installation Guide* for information on installing and deploying IdentityIQ.

Use the following IdentityIQ components to improve internal governance measures, optimize compliance efforts and more effectively manage risk.

- "Configure Applications" on page 89. — define the applications in your enterprise that will work with IdentityIQ. From this page you will specify the connection properties, relevant attributes, aggregation rules, and activity information for each application.

- "Entitlement Catalog" on page 93 — view and manage all of your managed attributes including; entitlements, account groups and permissions. From this page you can add new managed attributes and edit the existing manage attributes. You can also use this page to import list of managed attributes into IdentityIQ or export them back out to other applications.

- "Role Management" on page 91 — create and maintain roles and profiles that define your enterprise. These features, combined with information discovered from your application and user configuration, create the Identity Cubes that enable you to monitor and maintain compliance.

- "Group and Population User Interface" on page 99 — use the Group Configuration page to work with groups and populations within your enterprise. When these are enabled, activity can be tracked and monitored by membership and risk information, such as policy violations or risk scores.

- "Configure Activity Settings" on page 101 — create categories of targets, on multiple applications and data sources, for use in IdentityIQ activity searching.

- "Define Policies" on page 103 — define policies for your enterprise. Policies are comprised of rules used to enforce your policies.

- "Configure Risk Scoring" on page 105 — define the risk scoring model for use by IdentityIQ. IdentityIQ uses a combination of base access risk and compensated scoring to determine the overall risk scores, or composite risk score, used throughout the IdentityIQ application.

- "Business Process Editor" on page 107 — create and manage the workflows that are used throughout your enterprise. A workflow contains a sequence of steps or activities and each step can perform one or more actions.

- "System Setup" on page 109 — system setup options include login rules, identity mappings and system setting used throughout the IdentityIQ application.

IdentitiyIQ User Guide

Chapter 12: Configure Applications

You must define each application in your enterprise. Specify the connection properties, relevant attributes, targets and aggregation rules for each application. Configuring applications requires advanced knowledge of IdentityIQ, the other products with which IdentityIQ will communicate, and the operations of your enterprise.

For information on configuring your applications, refer to the *SailPoint IdentityIQ Application Configuration Guide* in your `IdentityIQ_InstallationDirectory\doc\pdf` directory.

For information on configuring your connectors, refer to the *SailPoint Direct Connectors Administration and Configuration Guide* found in your `IdentityIQ_InstallationDirectory\doc\pdf` directory.

Chapter 13: Role Management

Use Role management to create and maintain the roles that define your enterprise. These roles are used to:

- Categorize and manage users based on job function
- Provide a translation between business and IT functions
- Ease the provisioning and the request process for new access
- Simplify auditing and the access and certification process

Roles are an important part of an identity control system. Roles enable business managers to make more accurate decisions and to make an appropriate trade-off between business benefits and risks. Roles make it easier to translate business process rules into technical IT controls. Roles enable better visibility into IT data and provides metrics that business managers and executives can understand and approve.

For detailed information, refer to the *IdentityIQ Role and Group Management Guide* located in your `IdentityIQ_InstallationDirectory`\doc\pdf directory.

Role Management Concepts

Role mining analyzes data in the system using pattern-matching algorithms. You can use the results to help determine what new roles to create. IdentityIQ supports role mining to create both business and IT roles. Business roles typically model how users are grouped by business function, including functional hierarchies, project teams, or geographic location. IT roles typically model how application entitlements (or permissions) are logically grouped for streamlined access.

Business role mining in IdentityIQ facilitates the creation of organizational groupings based on identity attributes, for example department, cost center or job title. The business role mining supports multiple configuration options to assist users in generating new roles. After the mining task is completed, the new roles are added to the Role Viewer where they can be modified as necessary.

IdentityIQ also supports the creation of roles based on the mining of entitlements in the enterprise. These roles typically model the IT privileges required to perform a specific function in an application or other target system. Using a configurable algorithm, IdentityIQ searches for access patterns to determine logical groupings of entitlements.

When you define roles based on entitlements from the applications that IdentityIQ monitors, the aggregation and correlation process discovers the entitlements, matches them to the roles you defined, and assigns those roles to the users that have those entitlements. If you create a hierarchical structure of roles using the inheritance function of the Role Viewer, users are assigned the lowest level role discovered during aggregation. For example, if role A is a member of role B, and role B is a member of role C, and an identity is discovered that is assigned all of the entitlements that defined roles C, B, and A, they are assign role A. Assigning the lowest level role enables operations such as certifications to be performed on one role instead of on each entitlement assigned to the user.

Role type is used to configure roles to perform different functions in your business model. For example, type might be used to control inheritance or automatic assignment of roles. Role types are configured on the Global Configuration page (accessed via the **gear** menu > **Global Configuration** > **Role Configuration**).

Role management also uses the concept of permissions to enable you to grant users permission to certain roles without assigning them the role or incorporating it in their role hierarchy. For example, while a non-IT user with a business-type role might need access to the entitlements contained in an IT-type role, they probably do not need to have that role assigned to them or included as part of their hierarchal role structure.

Role archiving enables you to store versions of roles that have changed over time. This function enables you to roll-back to previous versions of the role if necessary. If roll approval is required in your enterprise, role roll-backs also require approval. Role archiving is controlled through business processes and is enabled during the configuration of the IdentityIQ product.

Role activation events enable you to use business processes to automatically activate or deactivate roles based on dates specified in the role modeler. Role activation business processes can be configured to automatically refresh identities to include or exclude the affected roles.

Chapter 14: Entitlement Catalog

Note: **The terms account group and application object are use interchangeably in this document but have the same meaning. Some application can have multiple application objects. An account group can be the name of one of those objects.**

Use the Entitlement Catalog page to view and manage all of your managed attributes including; entitlements, account groups/application objects and permissions.

Managed attributes can be specific to one application or shared among multiple applications of the same type. Managed attributes can also be defined in multiple languages.

A managed attribute is the value of an account attribute that has been promoted to a first-class object in the IdentityIQ database so the system can track other data related to these attributes, for example a description or an owner. Any attribute can become managed, but the most common attribute to be managed is one holding group memberships.

A managed attribute is indicated by checking the **Managed** box in the account schema on the Application Definition page.

As accounts are aggregated IdentityIQ detects the values for each managed attribute and promotes these to ManagedAttribute objects. For example if location is managed, and we aggregate three accounts with locations Austin, Dallas, and Houston. There are three ManagedAttribute objects for those values. If the attribute is multi-valued, such as groups or memberOf, IdentityIQ creates one ManagedAttribute for each value in the list.

The expectation is that most of the attributes that are managed are entitlement attributes, which usually means a group attribute. Because of this, the language in the product is oriented around the word entitlement. For example we refer to manage entitlements and the entitlement catalog. It is possible, however, to have managed attributes that are not entitlements, but it is unusual.

Managed attributes that are also groups have additional features. If the connector supports group aggregation, IdentityIQ can import the definitions of those groups and store them in the ManagedAttribute object. Managed attributes for groups have editable tabs that contain the definition of the group that can, optionally, be used for provisioning. If a groups managed attribute is available for provisioning, any change made on the Object Properties tab is sent to a connector to modify the target application.

Note: **The additional Object Properties tab is only available if Lifecycle Manager is installed and the Enable Account Group Management options was selected during Lifecycle Manager configuration.**

View Entitlement Catalog

From this page you can add new managed attributes and edit the existing manage attributes. You can also use this page to import lists of managed attributes into IdentityIQ or export them back out to other applications.

-

Table 1— Entitlement Catalog List

Column	Description
Application	The application to which the managed attribute belongs.

Column	Description
Attribute	The attribute (in the case of an Entitlement or Group) or target (in the case of a Permission) that the managed attribute represents.
Display Name	Display name of the managed attribute. If no display name was defined, this field displays the value of the attribute.
Name	The raw attribute value for the managed attribute. This column is hidden by default.
Type	The type of managed attribute that is shown. There are two types: Entitlement and Permission. However, entitlements can be marked with the boolean group property if they represent a group object type for the application. Since applications can have more than one group object type, the object type name, for example Group or Role, is shown here for those managed attributes.
Description	The description for the locale that is specified in the combination box between the search area and the grid.
Owner	The Identity who owns the managed attribute.
Requestable	Any managed attribute that can be requested has a check icon in this column.
Last Refreshed	The date and time that the managed attribute was last modified. This column is hidden by default.

Import and Export

Use the **Import** and **Export** buttons to import new managed attributes from a CSV file or export existing managed attributes to a CSV file. Each option opens a dialog with instruction on how to continue. The import and export processes are handled with tasks in IdentityIQ and can be tracked on the Tasks Results page.

The import data file is in a CSV format defined by comments at the top of the file. A comment line containing a comma-separated set of values defines the properties corresponding to the CSVs on subsequent lines. The imported Entitlements' properties will be set accordingly.

The properties on this line can be any of the following:

- application
- attribute
- value
- displayName
- requestable
- owner
- scope

Here is an example of this type of comment:

```
# value, displayName
```

A line containing an assignment statement defines default values for the imported Entitilements' properties.

Here is an example of this type of comment:

```
# application=Active_Directory
```

For importing attribute descriptions, you must also declare the language used. To get an example of the description format do the following:

1. Go to the Entitlement Catalog page, Applications->Entitlement Catalog.

2. Click **Export**.

3. Choose and application to Export.

4. Choose **Descriptions** from the Export Type drop-down list.

5. Choose the language in which to display the descriptions from the Choose description languages to export.

6. Click Export.

A message is displayed at the bottom of the browser window when the export is complete and from there you can view or save the exported descriptions.

Add or Edit Entitlement Parameters

Note: **You can only add new managed attributes of type entitlement.**

The edit page enables you to change properties on a managed attribute. The **Save** button at the bottom of the page kicks off a business process that persists the changes to the managed attribute. The title and content of this page varies depending on the type of attribute being edited. If necessary the business process kicks off provisioning. The Edit page can be accessed by clicking **New Entitlement** or clicking on an existing managed attribute from the list.

Deleting a managed entitlement does not directly remove the entitlement from the product. Instead a group update business process is launched as a task.

Track the progress of this task through Setup -> Tasks -> Task Results tab.

Standard Properties

The Standard Properties tab is common to all managed attributes regardless of type.

Table 2—Edit Managed Attribute Standard Properties Tab

Field	Description
Application	The application associated with the attribute.
Type	Application object type.
Attribute	**Note: This field is read-only when editing an existing managed attribute.** This field has different behavior based on the selected type: **Entitlement** - this field is labeled, **Attribute**, and the input is a suggest box populated with all attributes in the selected application's account schema. **Group** - this field is also labeled, **Attribute**, but no input choice is provided. The attribute is set to the reference attribute defined in the application's group schema. **Permission** - this field is labeled **Target** and the input is a free-form text box.

Table 2—Edit Managed Attribute Standard Properties Tab

Field	Description
Value	**Note: This field is only displayed for groups and entitlements. This field is read-only when editing an existing managed attribute. For groups with provisioning enabled, this field contains information on how the value was derived.** The attribute value represented by the managed attribute.
Display Value	**Note: This field is only displayed for groups and entitlements.** The value used to concisely represent this managed attribute in IdentityIQ. In many cases, this is the same as the value. Sometimes (when the value is an LDAP domain, for instance) this only contains a small, relevant portion of the value. No provisioning is launched when this field is changed.
Requestable	**Note:** This option is only displayed if you have SailPoint Lifecycle Manager enabled. Indicates whether or not the entitlement can be requested from the Lifecycle Manager.
Description	A localized description. **Note: You must Save the description before changing languages to enter another description.** Use the language selector to enter description in multiple languages. The drop-down list displays any languages supported by your instance of IdentityIQ. The description displayed throughout the product is dependent on the language associated with the user's browser. If only one description is entered, that will be the description used by default.
Owner	The owner of the managed attribute. No provisioning is launched when this field is changed.
Note: This tab might contain additional extended attributes that were defined as part of the configuration process. Extended attributes only apply to IdentityIQ's representation of the managed attribute and no provisioning is launched by them.	

Group Properties

This tab is only displayed for Group type managed attributes. This tab has three sections: Group Attributes, Hierarchy, and Permissions. To edit the fields on the tab, you must have the required rights and capabilities and the following condition must be met:

- Lifecycle Manager must be enabled.
- Lifecycle Manager must be configured to enable group provisioning.
- Group provisioning must be enabled for this managed attribute on the application with which it is associated.

If all of these conditions are not met, the tab is read-only.

Group Attributes:

Group attributes correspond to the attributes defined in the application's group schema. The EditGroup form defined on each application's Provisioning Policies tab is rendered onto this tab. If no such form is found, a default form is generated containing read-only representations of all the fields found in the application's group schema attributes.

Hierarchy:

> **Note:** This section is not displayed if the criteria are not met.

This section contains a multi-suggest list that enables you to add groups that can be inherited. The multi-suggest list contains only the managed attributes that meet the following criteria:

- The managed attribute is of type Group.
- The selected application has a non-null Group Hierarchy Attribute set in its configuration.

Permissions:

This is a read-only grid that lists all of the Permissions set on the managed attribute. This tab only pertains to Group and Permission type managed attributes.

Members

This is a read-only tab that lists all of the Identities with detected roles with profiles that match the edited managed attribute. This tab only pertains to Group type managed attributes.

Access

This is a read-only tab that lists any effective access for the entitlement.

Classifications

This tab lists any classifications that have been assigned to the entitlement. Classifications flag and categorize entitlements, most typically to identify entitlements that permit access to sensitive or protected data such as financial, personal, or health-related information. You can also add and remove classifications on this tab.

To add classifications to the entitlement, choose the entitlement(s) from **Assign Classifications to this Entitlement** and click **Add**. You can add as many classifications to the entitlement as you wish.

To remove classifications from the entitlement, check the classifications to remove, then click **Remove Selected**.

Add or Edit Entitlement Parameters

Chapter 15: Group and Population User Interface

Use the Group Configuration page to work with groups and populations in your enterprise. When groups and populations exist, you can track and monitor activity by membership and risk information, such as policy violations or risk scores.

To access the Groups page, navigate to **Setup > Groups**.

The Group Configure page has the following tabs:

- Groups — used to track accessibility, activity, and monitored risk by group membership. Risk scores are displayed on the Home Page. Groups are defined automatically by values assigned to identity attributes.
- Populations — are query based groups created from the results of searches run from the Identity Search page. Searches that result in interesting populations of identities can, optionally, be saved as populations for reuse within IdentityIQ.
- Workgroups — are groups of users in IdentityIQ that can perform actions, such as approvals, or own objects, such as roles or policies, within the system.

For detailed information, refer to the *IdentityIQ Role and Group Management Guide* located in your `IdentityIQ_InstallationDirectory\doc\pdf` directory.

Groups

Groups are defined automatically using values that are assigned to identity attributes such as Department, Location, Manager and Organization.

Groups associated with identity attribute values are defined using the values that are assigned to those attributes. For example, the Location identity attribute can have a value for each city in which your enterprise has an office, such as Austin, New_York, and London. In that case, there are three groups created, Austin, New_York, and London, one for each value of the attribute, and each contains the identities that have the corresponding value that is assigned to Location.

Populations and Workgroups

Populations are query based groups created from the results of searches run from the Identity Search page. Searches that result in interesting populations of identities can be saved as populations for reuse. Members of a population might not share any of the same identity attributes or account group membership. Population membership is based entirely on identity search parameters.

Workgroups enable the assignment of object ownership, certification, revocations and work items to pre-defined lists of identities. In addition to grouping Identities you are also able to assign capabilities and scope to these groups of identities so that you do not have to assign the same scopes and capabilities to each individual member of the group.

> Note: The tabs are empty until groups are defined and enabled.

-

Chapter 16: Configure Activity Settings

Use activity settings to customize activity tracking and monitoring in your enterprise. You can configure the activity settings to narrow the focus of activity searches.

The Activity Target Categories page displays a list of all of the defined categories to use with the Activity Search page. Activity Target Categories are groups of targets from one or more applications. For example, if you have inventory applications at three different locations and a procurement database on each, you can set each procurement database as a target, create a Procurement category, and then collect activity for all three procurement databases using a single activity search.

> **Note:** **Activity Data Sources and Activity Targets are defined when applications are configured to work with IdentityIQ. If no activity data source and targets were defined, you cannot create Activity Target Categories.**

Use the Activity Target Categories page to add or edit activity target categories.

Click an existing category or click **New Category** to open the Add Targets to Activity Category page and create or edit a category. To delete an active target category from the list, right-click on the category and select **Delete**.

For detailed information, refer to the *IdentityIQ System Adminstration Guide* located in your `IdentityIQ_InstallationDirectory`\doc\pdf directory.

Chapter 17: Define Policies

Use the Policies page to define policies for your enterprise. Policies are defined and used to monitor identities that are in violation of the policies. For example, a separation of duties policy can prohibit one identity from requesting and approving purchase orders. An activity policy can prohibit an identity with the Human Resource role from updating the payroll application even though the identity has view access to the application.

Rule violations for a policy, when detected, are stored in the Identity Cube. These violations also appear on identity score cards and enable you to identify high-risk employees and take appropriate action.

You can also configure violations to trigger a business process to send email notifications and generate work items so that policy violations can be managed immediately upon detection. Policy violations can be managed through certifications or the policy violations page.

- **Custom Policies —** are any policies that were created outside of IdentityIQ to meet special needs of your enterprise. You cannot create a custom policy from inside the product. Use the Edit Policy page to view information about a custom policy, but changes made here will not affect the performance of the policy.
- **SOD** – separation of duties policies ensure that identities are not assigned conflicting roles.
- **Entitlement SOD** — separation of duties policies ensure that identities are not assigned conflicting entitlements.
- **Effective Entitlement SOD** — separation of duties policies similar to the Entitlement SOD policy, but specifically for effective entitlements.
- **Activity** — ensure that users are not accessing sensitive application if they should not or when they should not.
- **Account** — ensure that an identity does not have multiple accounts on an application.
- **Risk** — ensure that users are not exceeding the maximum risk threshold set for your enterprise.
- **Advanced** — custom policies created using match lists, filters, scripts, rules, or populations.

To access Policies, navigate to **Setup > Policy**.

Policy Page

You can define and use policies to monitor identities that are in violation of the policies.

Managing Policies — To create a new policy, select a type from the **New Policy** drop-down menu. To edit an existing policy, click the policy row in the table or right-click the policy and select **Edit** from the drop-down menu. To remove a policy, right-click on the policy and select **Delete** from the drop-down menu.

Viewing Policy Violations — You can use filtering to limit the number of violations displayed. Filter by username, click **Advanced Search** to filter by policy type, or use a combination of the two. Click **Clear Filter** to repopulate the list with all of policy violations. To sort the information in the table by ascending or descending order, click the table header.

The Policies page has the following information:

Table 1—Policies Page Column Definitions

Column Name	Description
Name	The name of the policy assigned when it was defined.

Table 1—Policies Page Column Definitions

Column Name	Description
Type	The type of policy. **Role SOD** – separation of duties policies ensure that identities are not assigned conflicting roles. **Entitlement SOD** — separation of duties policies ensure that identities are not assigned conflicting entitlements. **Effective Entitlement SOD** — separation of duties policy for effective access, to ensure that identities are not assigned conflicting effective entitlements. **Activity** — ensure that users are not accessing sensitive application if they should not or when they should not. **Account** — ensure that an identity does not have multiple accounts on an application. **Risk** — ensure that users are not exceeding the maximum risk threshold set for your enterprise. **Advanced** — custom policies created using match lists, filters, scripts, rules, or populations.
Description	A brief description of the policy as entered when it was defined.
State	The status of the policy. **Active** — the policy is currently being used. **Inactive** — the policy is not being used.

For detailed information, refer to the *IdentityIQ Policy Management Guide* located in your *IdentityIQ_InstallationDirectory*\doc\pdf directory.

Chapter 18: Configure Risk Scoring

Use the risk scoring configuration pages to define the algorithms that IdentityIQ uses to determine risk scores for

identities and applications in your organization. Risk scores are used throughout the product to highlight high-risk users and accounts and trigger notices when configured to do so.

IdentityIQ uses a combination of base access risk and compensated scoring to determine the overall Identity Risk Scores or Composite Risk Score used throughout the product.

Base access risk is a measure of inherent user access risk. Base risk scores are set on each role, entitlement, and policy defined. This type of score ranges from 0 (lowest risk) to 1000 (highest risk). The account weight assigned to any additional entitlements assigned to an identity also affects base risk scores. Account weights are factored in to the entitlement baseline access risk scores.

Configuring risk scoring requires the assignment of administrative capabilities within IdentityIQ. For detailed information on configuring activity targets, refer to the *IdentityIQ System Administration Guide*. The Administration Guide is located in your `IdentityIQ_InstallationDirectory\doc\pdf` directory.

Access Risk Scoring Definitions

Use the risk scoring configuration pages to define the algorithms that IdentityIQ uses to determine risk scores for identities and applications in your organization. There are a number of scores, or types of scores, that contribute to the overall Identity Risk Score, or Composite Risk for each IdentityIQ user.

IdentityIQ applies a series of compensating factors to each base risk score to calculate compensated scores. These compensated scores are then weighted using a maximum contribution percentage and combined to form an overall Composite Risk Score for each user.

The compensating factors and weighted values enable IdentityIQ to accurately identify high risk users based on more than just the roles they are assigned within your enterprise.

For example, a user assigned only low risk roles may be considered high risk if they were never included in a

certification process or the roles they do have are in violation of separation of duty policies.

Table 1—Access Risk Scoring Definitions

Score	Definition
Base Risk Score	The score assigned to each role, entitlement, or policy violation.
Total Base Risk Score	The total score of all base risk scores of the same component type on a per user basis. For example, add the base risk scores for all roles assigned to a specific user together to determine the role total base risk score.
Compensated Risk Score	The value of the base risk score for a component multiplied by the compensating factor for that component type.
Total Compensated Risk Score	The Total Base Risk Score for a specific component type multiplied by the Compensated Risk Score for that component type.

Table 1—Access Risk Scoring Definitions

Score	Definition
Composite Risk Score or Identity Risk Score	The overall risk score for a user after the composite weighting, or maximum contribution to total score factor, is applied to the total compensated risk scores for each component. The time since the last certification was performed on the user can also figured into this score with the total compensated scores for role, entitlement, and policy violation.

Chapter 19: Business Process Editor

A business process contains a sequence of steps or activities and each step can perform one or more actions. Moving from one step to another is called a transition and transitions can be conditional based on the results of prior actions. When a business process is running it can open work items to handle human interaction. The business process maintains a set of variables that can change as the steps execute. Variables can be copied into work items to convey information to an approver and copied from work items to assimilate responses from the approver.

Business processes are not normally launched directly like tasks or reports. Instead they are launched as a side effect of some IdentityIQ operation such as editing a role, updating an identity, or the discovery of a policy violation. You cannot schedule a business process through the task or report scheduler, though you can schedule a custom task that launches a business process.

Immediately after launching, the business process engine begins interpreting or executing the business process. The starting step is located and its action is performed, the transitions are evaluated and the next step is located. This process continues until a step is found with an approval action or the end of the process is reached.

When the business process advances to a step containing an approval, work items are created and the business process enters a suspended state. The business process remains suspended until one of the work item owners completes the work item. Completing a work item is normally done by editing it in the IdentityIQ user interface and clicking one of the default completion buttons. Each work item can also control how its information is presented, and can include forms to solicit additional information from the user beyond just an approval or rejection decision.

An approval action can define a sequence of user interactions that are managed automatically by the business process engine. The work related to notifications, reminders, escalation, and sequencing from one approver to another is all handled by the business process engine rather than being modeled as steps in the business process. This provides a concise way to define one of the most common parts of a business process.

When a work item is completed, the business process uses the information from the work item to influence the transitions between steps. The work item also contains a State value which can be Finished, Rejected, Returned, or Expired. This state is used by the business process engine to decide whether to continue advancing through the approval process or to stop and go on to the next step. It might be found that work items previously sent to users are no longer required and they are automatically deleted.

If the approval process continues, more work items might be generated and the business process will again enter a suspended state. Once the approval process terminates, the transitions in the step containing the approval are evaluated and a new step is chosen. The evaluation of steps and transitions continues until another approval is reached or until all of the steps are evaluated and the business process terminates.

One unique aspect of this business process system is that the process can be modified during execution. This is done to adapt to variability in the approval process, such as an unknowable number of approvers, or an unknowable number of phases in an approval sequence. Self-modification can also be used in custom actions to replicate a sequence of steps for an unknowable number of objects. Since a copy of the original business process definition is maintained, modifying it during execution does not effect the persistent definition used when launching it again. Similarly, the original business process definition can be modified at any time without disrupting business processes that are already executing.

For detailed information, refer to the *IdentityIQ System Adminstration Guide* located in your `IdentityIQ_InstallationDirectory\doc\pdf` directory.

IdentitiyIQ User Guide

Chapter 20: System Setup

You can configure system-wide default settings for the entire IdentityIQ product, including features such as identity mapping, account mapping, role configuration, scopes, certification performance, the Lifecycle Manager settings (if you have purchased that product), and more.

To set up up global configuration options for IdentityIQ, click the **gear icon** on the Navigation menu bar and select from the list of options:

- Global Configuration
- Compliance Manager
- Lifecycle Manager

For detailed information, refer to the *IdentityIQ System Configuration Guide* located in your `IdentityIQ_InstallationDirectory\doc\pdf` directory.

Section III Using IdentityIQ

Use the following components to improve internal governance measures, optimize compliance efforts and more effectively manage risk.

- "Getting Started with IdentityIQ" on page 113 — get started by logging in to IdentityIQ using one of the various secure login methods that are available.

- "IdentityIQ Home Page and Navigation" on page 117 — a web-based console that enables you to review and act on compliance-related data and activities across the enterprise. The Home page displays after you log into the IdentityIQ or when you click the **Home** icon. The Home page functions as a dashboard with convenient links to specific areas IdentityIQ. These links are defined when IdentityIQ is deployed and are based on the needs of your enterprise.

- "Identity Management" on page 127 — monitor and access individual identity cube risk information. Identity Cubes are multi-dimensional data models of identity information that offer a single, logical representation of each managed user. Each Cube contains information about user entitlements, associated business context and historical records of user access configurations and activity.

- "Alerts" on page 141 —view and define alerts. The alerts list is view only, no action can be taken on alerts that have occurred within your system or the actions that those alerts initiated.

- "Tasks" on page 143 — automate the process of discovering users, assigning those users to contextual roles, and correlating these with user activity from log files to form Identity Cubes.

- "Advanced Analytics" on page 145 — create very specific queries on users, activity, and audit logging within your enterprise. These searches can be used to isolate specific areas of risk and create interesting populations of users from multiple organizations, departments and locations.

- "Manage Work Items" on page 175 — use the Manage Work Items page to view all work items that are assigned to you or to a workgroup of which you are a member and to view all work items assigned by you.

- "Policy Violations" on page 177 — manage policy violations outside of access certifications. This page enables you to identify policy violations within your organization as soon as they are detected and take action to rectify those violations immediately. Your system can be configured to notify policy owners or their delegates through email or work items each time a policy violation is detected by a regularly scheduled scan. Use this page to manage those violations instead of creating and running interim certifications manually.

- "Managing Application and Identity Risk Scores" on page 267 — Use the Identity Risk Score and Application Risk Score pages to view individual risk scores and the risk scores associated with each application.

- "Reports" on page 185 — locate stored reports, define parameters to run new reports, or submit ad hoc queries against the normalized data - to find answers to precise certification, application, role, user, policy, or activity questions.

IdentitiyIQ User Guide

Chapter 21: Getting Started with IdentityIQ

> **Note:** **Do not open multiple tabs or browsers. Opening multiple tabs might overwrite changes made in the other.**

> **Note:** **Based on your role and individual privileges, and how your system is configured some options in this section could be unavailable.**

How you log in to IdentityIQ is based on how your system is configured. The following login options can be available:

- Custom login
- "New User Registration" on page 113
- "QuickLinks" on page 94
- "Password Recovery - Account Unlock" on page 114

After you log in to IdentityIQ, the Home page displays. For more information, see "IdentityIQ Home Page and Navigation" on page 117.

New User Registration

Self service registration enables new users to request an IdentityIQ user account the first time they access the product. When this option is enabled, the **New User Registration** link displays below the **Password** field on the Welcome screen.

> **Note:** **To use this feature, enable Enable self-service registration on the Lifecycle Manager configuration page.**

> **Note:** **You can also access the New User Registration page through a direct link that bypasses the login page and simplifies the registration process.**

1. Click **New User Registration** link to launch the New User Registration page.

2. Fill in the required fields, which include the requested IdentityIQ user name and password.

3. Click **Register.**

After the request is authorized, you receive an email notification and you can use the name and password submitted to log on to IdentityIQ.

Multi-Factor Authentication

Multi Factor Authentication (MFA) adds an additional layer of security by requiring you to use multiple methods to authenticate your identity before you can log in to IdentityIQ. When MFA is configured for your system:

1. Log in to IdentityIQ from the default login page and then your MFA provider's login page displays. If your password is expired or you are required to change your password, you must complete the MFA process first.

2. Follow the login prompts for your provider.

3. After you are authenticated, you are logged in to IdentityIQ and the **Home** page displays.

    Note: **If you are assigned to multiple providers, you must select a provider from the provider list before you can proceed to the provider's login page.**

Password Recovery - Account Unlock

Based on the IdentityIQ configuration, the following options can be available:

- **Forgot Password** — your password is reset and you are automatically logged in to IdentityIQ
- **Account Unlock** — your account is unlocked and you can log in.

When an Administrator sets up password recovery and account unlock options, the following verification methods are configured:

- Answer Authentication Questions
- Send a Text Message with a Verification Code

Answer Authentication Questions

To use this feature, your administrator must activate this option and you must provide answers to authentication questions in your IdentityIQ User Preferences before this feature is available. See the IdentityIQ *User Guide* for more information.

Your administrator can set the following items that determine how you interact with this feature:

- Number of answers you must define in your IdentityIQ User Preferences.
- Number of correct answers you must provide to authentication questions.
- Maximum number of wrong answers you can enter before IdentityIQ locks you out.
- Number of minutes are locked out.

    Note: **To unlock the account before the lockout time ends, an administrator with the appropriate system capabilities can click Unlock Identity on the Identity Cube Attributes tab.**

How to Recover Your Password Using Authentication Questions

    Note: **If you have not set up and answered the authentication questions and do not know your password, you must contact your help desk or your IdentityIQ administrator to reset your password.**

Complete the following steps:

1. Click the **Forgot Password?** link.

2. Enter your username and click **OK**.

3. Enter the correct answers to the questions you previously set up and click **Done**.

    The responses entered on this window are compared to the recorded answers. If you provided the required number of correct answers, IdentityIQ can authenticate you. The authentication process ignores case when comparing the your answers to the stored answers.

4. On the next window, enter your new authentication password in the **New Password** and **Confirm Password** boxes and click **Change**.

Note: The new password must meet the requirements of the password policy that your IdentityIQ
administrator set up.

Send a Text Message with a Verification Code

To use this feature, your administrator must activate this option and a mobile telephone number must be
configured for your IdentityIQ account. Your mobile phone number must contain a complete number

including the area code.

Chapter 22: IdentityIQ Home Page and Navigation

> **Note:** **Lifecycle Manager must be installed to access the Lifecycle features. Contact your SailPoint representative for more information.**

> **Note:** **Based on your role and individual privileges, the availability of IdentityIQ components can be limited.**

The IdentityIQ Home page is a web-based console that enables you to review and act on compliance-related data and activities across the enterprise. The Home page displays after you log into the IdentityIQ or when you click the **Home** icon. The Home page functions as a dashboard with convenient links to specific areas IdentityIQ. These links are defined when IdentityIQ is deployed and are based on the needs of your enterprise.

This section has the following topics:
- "QuickLinks" on page 117
- "Home Page Widgets" on page 120
- "Navigation Menu Bar" on page 122

QuickLinks

QuickLinks are tasked-based links to frequently-used areas of IdentityIQ. Your administrator determines the behavior and availability of these links. QuickLinks are displayed as cards on the IdentityIQ Home page and as links in the QuickLink Menu, which is available throughout the product.
- "QuickLink Menu" on page 117 — Lists all of the QuickLinks that are available to the user. The menu is displayed on every IdentityIQ page. Your administrator can configure these links.
- "QuickLink Cards" on page 119 — Displays task-oriented based on available QuickLinks. Cards are available only on the Home page. Users can add or delete cards from their Home page.

QuickLink Menu

> **Note:** **For a QuickLink menu item to be available, a QuickLink must be configured. Based on your role and individual privileges, the availability of IdentityIQ QuickLinks can be limited.**

The QuickLink menu is available from any IdentityIQ page and provides access to frequently-used items. To view the QuickLink menu, click the QuickLink icon, the three-bar icon located on the Navigation menu. By default, IdentityIQ ships with the following QuickLink configuration in the QuickLink menu:

Table 1—QuickLink Menu Items

Type	Link	Description
My Tasks	Access Reviews	Links to Certifications -> My Reviews page that lists your current access reviews. Click an access review in the list to display the Access Review Details page.
	Approvals	Links to Manage Work Items page where you can view and manage approvals that are assigned to you or to a work group of which you are a member. You can also view approvals assigned by you.
	Forms	Links to Manage Work Items page where you can view and provide needed information for form work items.
	Signoff Reports	Links to Manage Work Items page where you can view and manage sign off report work items.
	Policy Violations	Links to Policy Violations page where you can view and manage policy violations outside of certifications.
Manage Access **Note: Requires Lifecycle Manager**	Manage User Access	Links to the Manage My Access page where you can request to add access based on roles or entitlements or remove access. If you can request access for others, the Manage User Access page displays.
	Manage Accounts	Links to the Manage Accounts page for yourself where you can double-click on a current account to make changes. If you can manage accounts for others, this option links to a page that lists identities. Double-click on an identity and select the account you want to manage.
	Change Password	Links to the Manage Passwords page for yourself where you can manage passwords for your current application accounts. If you can change passwords for others, this option links to a page that lists identities. Double-click on an identity to manage passwords for the identity's application accounts.
	Track My Requests	Links to Access Request page that lists your open access requests. to view details about a specific request double-click a listing.

Table 1—QuickLink Menu Items

Type	Link	Description
	Privileged Account Management	Links to the Privileged Account Management page. The SailPoint IdentityIQ Privileged Account Management Module (PAM) extends identity governance processes and controls to highly privileged access, enabling you to centrally manage access to privileged and non-privileged accounts. Talk to your SailPoint representative or refer to the SailPoint IdentityIQ Privileged Account Management Module Guide for more information.
Manage Identity **Note: Requires Lifecycle Manager**	Create identity	Links to the Create New page where you can create a new identity to be stored in the Identity Warehouse.
	Edit identity	Links to the Edit Identity Attributes page for yourself where you can specify and request changes to your identity attributes. If you can edit identity attributes for others, this option links to a page that lists identities. Double-click on an identity to specify and request changes for the identity's attributes.
	View Identity	Links to the View identity page for yourself where you can view identity information. If you can view identity information for others, this option links to a page that lists identities. Double-click on an identity to view the identity's information. The View Identity page contains information about an identity's attributes, entitlements, and application accounts.

QuickLink Cards

> **Note:** **For a QuickLink card to be available, a QuickLink must be configured by the Administrator. Additionally, Lifecycle Manager must be installed to use to use the QuickLink cards for the Access Request component.**

QuickLink cards are based on the QuickLinks that are set up when IdentityIQ is deployed. You can re-arrange, move and add QuickLink cards on your Home page. See "How to Manage QuickLink Cards on Your Home Page" on page 120.

By default, IdentityIQ ships with the following cards set up on the Home page:

- Policy Violations
- Access Reviews
- Approvals
- Manage User Access
- Track My Requests

> **Note:** **To use the The QuickLink cards for the Access Request component Lifecycle Manager must be installed and a QuickLink must be configured.**

See "QuickLink Menu" on page 117 for more information for information about default QuickLinks.

How to Manage QuickLink Cards on Your Home Page

To make changes to your Home page, click **Edit** and make any of the following changes:

- Re-arrange cards — Click and hold **Drag** and then move the card to the new location.
- Remove a card — Click **Remove**.
- Add a card — Click **Add Card** and select one or items from the list of available cards and then click **Save**. to close the selection window.

> **Note:** You can also set the type of cards to display first, QuickLink cards or Quick View cards.

When your changes are complete, click **Save**.

Home Page Widgets

> **Note:** Based on your role and individual privileges, the availability of IdentityIQ Widgets can be limited.

Homepage Widgets use bite-size visualizations and data grids to present information of interest to the logged-in user. You can re-arrange, move and add widgets on your Home page. See "How to Manage Widgets on Your Home Page" on page 122. Click any item in the Quick View card to go to the stand-alone page associated with the card. Click **All** to view the stand-along page with all the listings associated with the card.

By default, IdentityIQ ships with the following predefined Widgets:

Table 2—Widgets

Type	Name	Description
Work Item	Latest Approvals	Displays the five most recent approvals that the logged-in user or one of their work groups.
	Latest Policy Violations	Displays the five most recent forms that the logged-in user or one of their work groups
	Latest Forms	Displays the five most recent forms that the logged-in user or one of their work groups.

Table 2—Widgets

Type	Name	Description
Certification	Certification Campaigns	To view this widgets, user must have compliance officer, certification admin, or auditor capabilities. Displays as a chart that indicates the completion status as a percentage.The color of the chart and message displayed under the title change based on the proximity to the due date. Today — Text indicates Due Today and chart is red. Week — Text indicates Due This Week and chart is orange. Other - Text indicates Due X where X is the due date and chart is green.
	My Access Requests	Displays as a pie chart that indicates the completion status as with the number of items completed out of total items. The color of the chart and message displayed under the title change based on the proximity to the due date. Today — Text indicates Due Today and chart is red. Week — Text indicates Due This Week and chart is orange. Other - Text indicates Due X where X is the due date and chart is green.
Risk	Risk Scores: Applications and Identities	Displays risk scores for applications and identities. By default, the Applications panel displays the top five applications with the highest risk scores. To view the top five identities with the highest risk score, click the forward arrow. To switch between the panels, click the forward or back arrow.
Productivity	Direct Report Actions	Displays a list of the direct reports for the logged-in manager. Based on the manager's rights and capabilities, the manager can perform actions such as request access, change password, manager accounts, and view identity details. Click and identity name to view information about the identity.
Data Governance **Note: Requires the File Access Manager integration**	Sensitive Data Exposure	Shows the number of overexposed resources, and the overall compliance score. The compliance score is color coded to indicate risk (0-5 is considered high risk, 5.1-7.5 medium risk, and 7.6-10 low risk).
	Sensitive Resources Missing Owners	Shows the number of resources with classified data that are missing an assigned data owner, and the overall compliance score. The compliance score is color coded to indicate risk (0-5 is considered high risk, 5.1-7.5 medium risk, and 7.6-10 low risk).

How to Manage Widgets on Your Home Page

To make changes to your Home page, click **Edit** and make any of the following changes:

- Re-arrange cards — Click and hold **Drag** and then move the card to the new location.
- Remove a card — Click **Remove**.
- Add a card — Click **Add Card** and select one or items from the list of available cards and then click **Save**. to close the selection window.

> **Note:** You can also set the type of cards to display first, QuickLink cards or Widgets.

When your changes are complete, click **Save**.

Navigation Menu Bar

> **Note:** Based on your role and individual privileges, the availability of IdentityIQ navigation menu bar items can be limited. Additionally, some options require IdentityIQ administrative capabilities. For information about setting up administrative capabilities, contact your IdentityIQ administrator.

The Navigation bar can be accessed from any IdentityIQ page and provides a convenient way to access areas of IdentityIQ. By default, IdentityIQ ships with the following top-level headings in the Navigation bar:

- "Home" on page 122
- "My Work" on page 122
- "Identities" on page 123
- "Applications" on page 123
- "Intelligence" on page 123
- "Data Governance" on page 124
- "Setup" on page 124
- "Gear Icon - Administration Menu" on page 125
- "Bell Icon - Work Item Menu" on page 125
- "User Name - User Menu" on page 125

Home

Your Home page functions as a dashboard with convenient QuickLink cards that link directly to frequently-used areas IdentityIQ Click **Home** in the Navigation menu bar from any IdentityIQ page to refresh or return to the Home page.

You can re-arrange, add or delete QuicklLink cards based on available QuickLinks. See "How to Manage QuickLink Cards on Your Home Page" on page 120.

My Work

This menu item links to the Manage Work Items page where your can view and manage open items that require your input, such as Access Reviews, Access Requests, Policy Violations and Work Items.

Identities

This menu item links to the The Identities page that contains links to pages related to user identities, such as:

Table 3—Identities: Menu Bar Link Descriptions

Link	Description
Identity Warehouse	Links to Identity Warehouse page where you can create, view and edit information for individual identities in your enterprise.
Identity Correlation	Links to Identity Correlation page where you can correlate one or more accounts with an identity.
Identity Risk Model	Links to Risk Scoring Configuration page where you can Configure risk scoring identities.

For more information, see the IdentityIQ *Administration Guide*.

Applications

The Applications menu bar item contains links to pages related to applications and entitlements, such as:

Table 4—Applications: Menu Bar Link Descriptions

Link	Description
Application Definition	Links to Application Definition page where you can specify the connection properties, relevant attributes, targets and aggregation rules for each application in your enterprise to work with IdentityIQ.
Entitlement Catalog	Links to Entitlement Catalog page where you can view and manage managed attributes including entitlements, account groups/application objects and permissions.
Application Risk Model	Links to Application Risk Scoring Configuration page where you can Configure risk scoring for applications in your organization.
Activity Target Categories	Links to Activity Target Categories page where you can view, add or edit the defined categories to use with the Activity Search page.

For more information, see the IdentityIQ *Administration Guide*.

Intelligence

The Intelligence menu bar item contains links to pages related to analytics, such as:

Table 5—Intelligence: Menu Bar Link Descriptions

Link	Description
Advanced Analytics	Links to Advanced Analytics page where you can create specific queries based on identities, certifications, activity and audit logs.

Link	Description
Reports	Links to Reports page where you can use standard or custom reports to collect information you need to manage the compliance process.
Identity Risk Scores	Links to Identity Risk Score page where you can view individual risk scores for users.The page displays one tab for each risk level defined in IdentityIQ.
Application Risk Scores	Links to Application Risk Scores page where you can view risk scores associated with each application. The page displays a table summarizing all of the applications score cards.

Data Governance

The Data Governance menu bar item is available only if the File Access Manager integration has been implemented, and is viewable only by users with an IdentityIQ capability that includes rights to see File Access Manager features. It contains links that provide direct access to the File Access Manager website.

For information about the Data Governance menu options, refer to the *IdentityIQ File Access Manager Administrator Guide*.

Setup

The Setup menu bar item contains links to pages related to configuration items, such as:

Table 6—Setup: Menu Bar Link Descriptions

Link	Description
Certifications	Links to Certifications page where you can view and create the scheduled certifications that are required to maintain compliance in your enterprise.
Roles	Links to Role Management page where you can create and maintain the roles that define your enterprise.
Policies	Links to Policies page where you can define policies to monitor identities that are in violation of the policies.
Tasks	Links to Task page where you can create tasks that automate the processes that build, update, and maintain the information contained within IdentityIQ.
Groups	Links to Group Configuration page where you can work with groups and populations that track and monitor activity by membership and risk information.
Business Processes	Links to Business Process Editor page where you can create a sequence of steps or activities and each step can perform one or more actions.
Lifecycle Events	Links to Lifecycle Events page where you can create new events or configure existing events in your enterprise to trigger business processes.
Batch Requests	Links to Batch Requests page where you can work with batch requests that enable you to generate specific types of access requests for more than one user at a time.

For more information, see the IdentityIQ *Administration Guide*.

Gear Icon - Administration Menu

> **Note:** **You must have IdentityIQ administrative capabilities to use this option. For information about setting up administrative capabilities, contact your IdentityIQ administrator.**

The Administration menu bar item contains links to pages specific to system-wide configurations, such as:

- Global Settings — Configure control and default settings for the entire IdentityIQ product.
- Lifecycle Manager — Adds tools, work items and reports related to Lifecycle Manager core functionality.
- Compliance Manager — Automates access certifications, policy management, and audit reporting.
- Administrative Console — Provides Task, Provisioning, and Environment monitoring tables.
- Plugins — Displays the third-party plugins configured to work with IdentityIQ.

For more information, see the IdentityIQ *Administration Guide*.

Bell Icon - Work Item Menu

> **Note:** **The count for work item types refreshes on a regular interval. By default, the refresh cycle is five minutes. Because your administrator can customize this setting, your refresh cycle can be different.**

The Bell icon provides notifications and quick access to work items for a logged-in user and can include the following types of work items:

- Approvals
- Forms
- Violations
- Others

When you log in, a red badge displays on the Bell icon and indicates the total number of any work items you have. Click a work item to display the associated Work Item page. See "Manage Work Items" on page 175.

User Name - User Menu

The name of the user is displayed in the navigation menu bar and contains links to pages specific to a logged-in user, such as:

- Preferences — Click to view or make changes to your user preferences. See "User Preferences" on page 125.
- Help — Click to access IdentityIQ online help.
- Logout — Click to log out of IdentityIQ.

User Preferences

Your your User Preferences includes settings that personalize how you use IdentityIQ. You can:

> **Note:** Only administration level users can change the name and email information.

- Specify your name, the email address to use for notifications.
- Set up a user to whom all work items assigned to you are to be forwarded.
- If a forwarding user is used, edit the Start and End Dates for all forwarded work items.
- Set the default view of identity-type certification requests.
- Change the password you use to log in to IdentityIQ.

The Edit Preferences page contains the following information:

Table 7—Edit Preferences Field Descriptions - General Tab

Field	Description
First and Last Name	Enter the first and last name to use for notifications.
Email Address	Enter an email address to use for notifications.
Forwarding User	Select a user who will receive all assigned work items assigned to you.
Start/End Date	Select the start and end date for forwarding work items.

Table 8—Edit Preferences Field Description - Password Tab

Field	Description
Current Password	Enter your current password.
New Password	Enter the new desired password.
Confirm New Password	Re-enter the new password to confirm.

Field	Description
Question # 1	Select question from the drop-down.
Answer #1	Type correct answer.

Chapter 23: Identity Management

Use the Identity Warehouse page to create, view and edit individual Identity Cube risk information. Identity Cubes are multi-dimensional data models of identity information that offer a single, logical representation of each managed user. Each Cube contains information about user entitlements, associated business context and historical records of user access configurations and activity.

IdentityIQ provides the following Identity Cube components:

- "Identity Warehouse Page" on page 1 — basic user information for every user in your organization.
- "Configure Risk Scoring" on page 105 — displays one tab for each risk level defined in IdentityIQ. Click on a tab to display a list of all of the users that fall into that risk level.
- "Identity Details Page" on page 128 — displays detailed information for one individual identity.
- "Identity Search" on page 145— generate searches on specific attributes of the users in your enterprise.
- "Manual Correlation of Identity Cubes" on page 136 — manually correlate the Identity Cubes created when identity aggregation was performed on your identity authoritative sources with any user accounts discovered while performing aggregations on other applications.

Access to components is controlled by IdentityIQ Capabilities and Scope. Contact your system administrator if you need access to additional components.

Identity Warehouse Page

The Identities table contains basic user information for every user discovered during the latest aggregation process.

Note: **By default, only active identities are displayed.**

Note: **Many columns in the table can be sorted. Click the column title to sort the table by the entries in that column in ascending order. Click again to sort the table in descending order. You can also click the associated drop-down menu to sort or to add or remove columns in the table.**

The Identity Warehouse page contains the following items:

Table 1—Identities Column Descriptions

Column Name	Description
Search	Enter a letter, or combination of letters, and click **Filter** to display users that have that letter combination in their name.
User Name	The user's account ID or login name.
First Name	Full first name of the user.
Last Name	Full last name of the user.
Manager	Name of the manager for the user.
Assigned Role Summary	A complete list of all roles assigned to the user.
Detected Role Summary	A complete list of all detected roles for the user.

Column Name	Description
Risk Score	The composite risk score for the user. Risk score is determined by numerous factors defined during configuration.
Last Refresh	The date of the last identity refresh.
Type	The type assigned to this identity, Employee, Contractor, External/Partner, RPA/Bots, or Service Accounts.
Location	The physical location of the user. For example, Chicago or Singapore.
Region	The corporate region assigned to the user. For example, U.S. or Asia-Pacific.

Click a user entry to display the View Identity page. Identity Details Page on page 128.

Identity Details Page

Use the View Identity page to view detailed information about each component of the Identity Cube for a selected user.

The Identity Details page contains the following option:
- "View Identity Attributes Tab" on page 145
- "View Identity Entitlement Tab" on page 146
- "View Identity Application Accounts Tab" on page 147
- "View Identity Policy Tab" on page 147
- "View Identity History Tab" on page 133
- "View Identity Risk Tab" on page 134
- "View Identity Activity Tab" on page 150
- "User Rights Tab" on page 133

"View Identity Events Tab" on page 138
-
-

Attributes Tab

The Attributes tab provides the basic user identity information such as first name, last name, and email, as well as enabling you to update the user password and the forwarding user, including the following fields:

Table 2—Identity Attributes tab Field Descriptions

Field Name	Description
Edit	Click to modify attribute values as needed, if available.
Manager	The manager to whom the user reports directly. Click the manager name to display the View Identity page for that user.

Table 2—Identity Attributes tab Field Descriptions

Field Name	Description
Change Password	Set or update a password for the user. Select the check-box below the password confirmation field to require the user to change their password the next time they log in to IdentityIQ.
Change Forwarding User	Change the user to whom work items assigned to this identity should be forwarded. Optionally use the Start Forwarding and End Forwarding options to set a specific time period in which forwarding should occur.

Entitlements Tab

The Entitlement tab lists all of the roles and entitlements for the selected user.

The Entitlement tab contains the following information:

Table 3—Entitlements tab Field Descriptions

Field Name	Description
Roles	A list of roles that were detected or assigned to the user manually or through role assignment rules. Assigned roles are typically business-type roles that model how users are grouped by business function, including functional hierarchies, project teams, or geographic location. Detected roles are roles that are detected by IdentityIQ during the aggregation and correlation processes based on the entitlements assigned to an identity. If an activation or deactivation date is defined for the role it is displayed in a message box below the role name. **Name** — name of the role. Click the name to view detailed information about the role. **Description** — brief description of the role. **Classifications** — if the role has a classification that categorizes it as potentially allowing access to sensitive, protected, or otherwise significant data, an icon is shown to flag the classification **Assigned By** — the user that assigned this role to the identity being viewed. **Allowed By** — the assigned roles that permit a user to have this role, either directly or indirectly. A direct permission is one in which the assigned role is a member of the permitted role. An indirect permission is one in which the assigned role is on the permitted list for the assigned role. **Acquired** — how the role was acquired. **Application** — the application associated with the role. **Account Name** — the application account the role is mapped to.

Table 3—Entitlements tab Field Descriptions

Field Name	Description
Entitlements	A list of the applications that have entitlements to which the identity has access. Click the entitlement or application name to view the entitlement details, if available. When an information icon is displayed, you can hover over it to view more details. If the entitlement has a classification that categorizes it as potentially allowing access to sensitive, protected, or otherwise significant data, an icon is shown to flag the classification Select **Show only additional entitlements** to limit the list to entitlements that are not included in a role assigned to the user

Application Accounts Tab

The Applications Accounts tab lists account information for all of the applications to which the user has some level of access. Click an application name to view detailed information.

Select an account in the table and click **Delete** to remove the link between the identity and the application in IdentityIQ. This action does not affect the user's account or entitlements on the application.

To transfer the account to a different identity, select an account and click **Move Account**. On the Select Account Owner dialog, select an existing identity from the list or create a new identity. To select an existing identity enter the first few letters of the identity name to display a suggestion list, or click the arrow next to the field to display a list of all identities to which you have access.

The Accounts link contains the following information:

Table 4—Identity Attributes tab Column Descriptions

Column Name	Description
Application	The name of the applications to which the user has some level of access. Click on an application name to view detailed information.
Account Name	The simple name used to identify the user on the application.
Status	Values can include: **Disabled** - the account has been disabled by an admin at some point. **Locked** - the user is locked out after too many password attempts. **Active** - the account is not disabled or locked.
Last Refresh	Date on which the user identity information was last refreshed.

Policy Tab

The Policy link lists policy violations for the user. The table contains the policy and rules that are violated.

Policies are composed of rules used to enforce your organization's policies. For example, a separation of duty rule might be defined that disallows a single user from having roles that enable them to both request and approve purchase orders.

The Policy link contains the following information:

Table 5—Identity Policy tab Column Descriptions

Column Name	Description
Detected	The date when the policy violation was detected.
Policy	The policy that is violated.
Policy Violation Owner	The owner of the policy. The owner is assigned during the policy definition process.
Rule	The specific rule that is being broken to cause the violation in the policy. Click a rule to display the following rule information: **Policy Description** — brief description of the violation as defined with the policy. **Policy Violation Owner** — the owner of the policy with which you are in violation. **Rule Description** — brief description of the rule from the rule definition page. **Compensating Control** — any compensating controls associated with this rule. **Correction Advice** — advice on how to correct the violation as entered when the rule was created.
Summary	The reason for the violation.

History Tab

The History link provides a history of user data. Tracking identity scores over time enables you to identity patterns or trends in the activity of a selected user.

The History link contains the following information:

Table 6—Identity History tab Column Descriptions

Column Name	Description
Identity Snapshots	
Snapshot Date	The dates of the identity snapshots. The frequency with which snapshots are generated is set on the Configure Systems Settings page. Click on a shapshot date from the table to display the View Identity History page.
Roles	A list of the roles that are currently assigned to this user.
Identity Certification History	
Decision	Displays an icon that indicates the decision made on the certification. Options include Approved, Revoked, Allowed Exception, or Delegated. For detailed descriptions of decisions, see "Certification Overview" on page 3.
Type	The type of certification. For example, Role or Additional Entitlement.
Description	Brief description of the certification.
Application	The application to which the certification applies.

Table 6—Identity History tab Column Descriptions

Column Name	Description
Account Name	The account name to which the certification applies.
Actor	The person who signed off on the certification.
Date	The date when the certification decision was made.
Comments	Any comments entered during the decision phase of the certification.

Click any row in the Identity Certification History panel to see an overview of that specific portion's certification history.

View Identity History Page

The View Identity History page contains user information from the specific date and time listed on the top of the page.

The View Identity History page contains four tabs:

- Attributes — the identity attributes.
- Roles — roles assigned to this user and all of the associated entitlements.
- Extra Entitlements — all entitlements assigned to this user that are not part of a role assigned to the user.
- Application Accounts — all applications on which this user has an active account, along with the account name, and the user's full identity.

Risk Tab

The Identity Risk Tab provides a current composite identity risk score with a list of the raw and compensated risk score for each category used to derive the composite score. This page also provides a list of the top composite score contributors which provide further information on how the score was derived. This information helps to provide clues on the areas of highest risk. These scores are based on the latest information discovered.

IdentityIQ uses a combination of base access risk and compensated scoring to determine the overall Identity Risk Scores, or Composite Risk Score, used throughout the application.

Base access risk score is a measure of inherent user access risk. Base risk scores are set on each role, entitlement, and policy defined. This type of score ranges from 0 (lowest risk) to 1000 (highest risk).

A series of compensating factors are applied to each base risk score to calculate compensated scores. These compensated scores are then weighted using a maximum contribution percentage and combined to form an overall Composite Risk Score for each user.

The compensating factors and weighted values enable you to identify high risk users based on more than the roles they are assigned in your enterprise.

-

Activity Tab

The View Identity Activity tab provides a list of all applications that have activity monitoring enabled and to which a user has access, the roles associated with those applications, and the activities performed.

The Recent Activities table initially lists the last ten (10) actions performed. Click **See All Activities** to include all of the activities stored by IdentityIQ on the table.

From this tab you can also enable activity monitoring for this user on specific applications that do not have activity monitoring enabled at the role level.

> **Note:** **Changes made to activity monitoring do not appear until identity aggregation is performed from the task page, or a scheduled identity aggregation takes place.**

To enable activity monitoring for this user on the associated applications and roles, select the **Activity Monitoring** check-box next to the Activities Settings table.

To display additional activity information in the Activity Details panel, click an activity entry in the Recent Activities list.

The View Identity Activity tab contains the following information:

Table 7—Identity Activity tab Column Descriptions

Column	Description
Activity Settings:	
Activity Monitoring Check-box	Enable activity monitoring for this user on the specified application. If this box is not active, activity monitoring is already enabled at the role level or the application does not allow activity monitoring.
Applications	The list of applications to which this user has some level of access.
Activity Enabled Roles	The list of roles that are all of the following: - assigned to this user - associated with the application - have activity monitoring enabled Activity monitoring is enabled when roles are defined.
Recent Activities:	
Date	The date on which the activity occurred.
Action	The activity performed on the application. For example, Login, Update, Delete.
Target	The specific part of the application that was targeted by the activity. For example, the name of a particular database that was updated.
Application	The application on which the activity was performed.
Result	The result of the activity. For example, Success or Failure.

User Rights Tab

The User Rights tab enables you to set the capabilities and define controlled scope for the user.

> **Note:** **The scope feature MUST be enabled in order for the scope information to display.**

Table 8—Identity User Rights tab Field Descriptions

Field Name	Description
User Capabilities	The SailPoint capabilities available. The capabilities currently assigned to the user are highlighted on the list. Contact your support representative for a full list of the Capabilities available. Use the Ctrl and Shift keys to select multiple capabilities.
Assigned Scope	The scope the identity belongs to.
Can Access Assigned Scope	Select this option to enable the identity to have access to the scope to which they are assigned. If this field is set to False, the user will not have access to objects within the scope to which they are assigned. If the field is set to Use System Default (<value>), the user's access is based on the value of the setting defined in the Global Settings for IdentityIQ.
Authorized Scopes	The scopes the user has access to. If scopes are active, identities can only see objects that are within the scopes they have access to. Assign scopes to the identity using the field at the top of the Authorized Scopes list box. • Click the arrow to the right of the field to display a list of all scopes defined. • Enter a few letters in the field to display a list of all scopes that start with that letter string. Depending on configuration, objects with no scope assigned might be visible to all users with the correct capabilities.
Workgroups	The workgroups to which this identity belongs
Indirect Rights	IdentityIQ capabilities assigned to a workgroup to which this user belongs. Workgroup members automatically have the capabilities and scopes assigned to the workgroup.

Capabilities Access

The capabilities an identity is assigned dictates which tools, pages, or tabs are accessible within IdentityIQ. To see the complete list of IdentityIQ default capabilities and their associated features, contact your support representative or log on to the SailPoint support Web site.

> Note: System Administrator has access to all IdentityIQ features including Global Settings, and Debug.

Events Tab

The Events tab enables you to view events that are scheduled for the user as well as detailed access request history.

The Events tab has two sections:

- "Events" on page 135
- "Access Requests" on page 135

Events

The Events list has two sections:

- Future Events shows scheduled role sunrise and sunset events.
- Past Events shows Identity Triggers and role sunrise/sunsets events that have been executed.

Select event and click **Delete** to cancel that event and remove the schedule from the list.

Table 9—Identity Events Descriptions

Field Name	Description
Created On	The date when the event schedule was created.
Created By	The identity that scheduled the event.
Due On	The date when the event is scheduled to occur.
Summary	A brief summary of the event that is pulled from the business process with which it is associated.

Access Requests

Click on a item in the list to display detailed information about requested items and any pending actions that still need to be taken on that request. From the detailed history panel you can navigate further into the request to expand the details view, review the actual access request, and send messages to owners of the request reminding them that their action is required.

Click the **X** icon to cancel a request.

To search for specific access requests, click **Search** to expand the search criteria. Specify the search criteria and click **Search**. To clear the criteria for a new search, click **Reset**.

Table 10—Access Requests Descriptions

Column Name	Description
Access Request ID	Identification number assigned to the access request.
Priority	Specifies the priority level to which the access request was designated.
Type	The type of access request.
Description	The a brief description of the access request.
Requester	The name of the user who assigned this work item to you.
Requestee	The name of the user who was assigned this access request.
Request Date	The date the request was made.

Table 10—Access Requests Descriptions

Column Name	Description
Current Step	Status of the request. Status levels include: Pending — Request was received but no action has taken place. Approved — Request was approved. Additional action may be needed to complete the request. Rejected — Request was denied. Completed — All actions required for this access request have been fulfilled. Cancelled — Request was cancelled. Completed Pending Verification — The manual action for this request was completed, however the verification procedure has yet to have been run.
Completion Date	The date when the work item was completed.
Execution Status	Status of the request execution. Status levels include: Executing — The request is going through the business process and has not completed. Verifying — The request has finished the business process and is waiting for the Provisioning Scanner to verify it. Terminated — The request was terminated before it was completed. Completed — The request was completed and verified.

Manual Correlation of Identity Cubes

Use the Identity Correlation page to maintain the IdentityIQ Identity Cubes which contain information about an individual user's entitlements, activity and associated business context. Identity Cubes are created when identity aggregation is performed on your identity authoritative source. An example of an identity authoritative source is a human resources application that is the main repository for employee information and the data source that is used to build most Identity Cubes.

> **Note:** **If user accounts are discovered on at-risk applications that do not correlate to the IdentityIQ identities that were created based on the employee information in your identity authoritative sources, it may indicate a risk situation that needs to be addressed.**

Because each Identity Cube is associated with an identity authoritative source, it provides a single representation of each managed identity and associated user accounts. However, user accounts on applications may not correlate to IdentityIQ identities. Some examples include the following:

- An employee who no longer works for your enterprise. They were removed from the human resources application, however, their account was not removed from every application to which they had access.
- Mismatched or redundant accounts. Accounts that were created on different applications at different times or by different administrators using variations of the employee's name; Tom Jones, Thomas Jones, and tjones.

To display detailed information about the account or identity, click an account ID or name. The details panels for an account and an identity can be open at the same time for comparison before you perform a merge.

Accounts that are manually assigned to identities from this page can be reassigned if necessary from the identity Application Accounts tab. See "View Identity Application Accounts Tab" on page 145.

Use the Correlated column of the Select Target Identity panel to manually change the correlation status of specific accounts.

The Identity Correlation page is divided into two panels:

- Select Uncorrelated Accounts — a list of the accounts on a specific application that are not correlated with an account detected on an authoritative source. See "Select Uncorrelated Accounts Panel" on page 137.
- Select Target Identity — a list of all accounts detected on all applications monitored by IdentityIQ. See "Select Target Identity Panel" on page 138.

Make selections in each panel to perform manual correlation. See "How to Perform Manual Identity Correlation" on page 138.

Select Uncorrelated Accounts Panel

The Select Uncorrelated Accounts panel displays a list of the accounts on a specific application that are not correlated with an account detected on an authoritative source. From this list you can select accounts to merge with identities.

Select an application from the **Search** drop-down list or enter the first few letters of an application name and make a selection from the suggest box to populate the table. Use the filtering options to reduce the number of accounts displayed at one time.

Use the Included Account Types filter to exclude specific account types from the uncorrelated list. For example, certain account types such as Service or Privileged accounts may never be assigned to specific users and, therefore, should never be correlated with a specific Identity Cube. To exclude a specific account type from the uncorrelated accounts list, click **Included Account Types** and clear the check-box associated with that account type on the drop-down list.

Click an Account ID to display detailed account information.

The Select Uncorrelated Accounts panel contains the ID and user name associated with the account and the date the account was created, along with the following options:

> Note: **The columns on this page can be configured and may display differently in your enterprise.**

Table 11—Identity Correlation - Uncorrelated Accounts Panel Descriptions

Column	Description
Account ID	Unique identifier associated with the account
Account Name	Name associated with the account.
Create Date	The date when the account was created.
Inactive Account	Inactive accounts have a value of true. This column can be used for account type filtering.
Last login	The date when the account was last accessed.
Service Account	Mark accounts as service accounts if appropriate. This column can be used for account type filtering.
Privileged Account	Privileged accounts have a value of true. This column can be used for account type filtering.

Select Target Identity Panel

The Select Target Identity panel contains a list of all accounts detected on all applications that IdentityIQ monitors. From this list you can select an identity with which to merge the uncorrelated accounts on the selected application.

Use the filtering options to display specific identities or click the filter icon to display every identity in IdentityIQ. Enter a letter string and click the search icon to search by user name or click **Advanced Search** for more options.

Click a Name to display detailed information about the selected identity.

The Select Target Identity panel contains the a variety of information about the identity, including the following:

> Note: **The columns on this page can be configured and may display differently in your enterprise.**

Table 12—Identity Correlation - Select Target Identity Descriptions

Column	Description
Correlated	The correlation status of the identity. Accounts marked as correlated no longer display on the uncorrelated accounts list or reports.
Manager	Manager listed for this identity.
Email	Full email address.
Inactive	Current status of the identity account, active or inactive.
Last Refresh	The date when the last identity refresh was performed on this identity cube.
Advanced Search Options:	
Standard Attributes:	
Standard attributes include name, username, email, and manager fields. Enter a letter string in any of these fields to return a list of identities that have a matching string in that identity attribute value. For example, typing st in the first name field returns Steve and Hester.	
Inactive	True - only show active identities False - only show inactive identities
Correlated	True - only show correlated identities False - only show uncorrelated identities
Searchable Attributes: Searchable attributes are defined during configuration and vary for each installation of the product.	

How to Perform Manual Identity Correlation

To perform identity correlation complete the following steps:

1. Click or mouse-over the **Identities** menu item and select **Identity Correlation**.

2. Select an application from the **Search** drop-down list or enter the first few letters of an application name and make a selection from the suggest box to populate the table. This table contains a list of the accounts on a specific application that are not correlated with an account detected on an authoritative source.

3. Select accounts to merge with identities that were created during the aggregation of your authoritative sources.

4. In Select Target Identity, select an identity to merge with the uncorrelated accounts selected in step 3. Use the filtering options to display specific identities or click the filter icon to display every identity in IdentityIQ. Enter a letter string and click the search icon to search by user name or click **Advanced Search** for more options.

5. Select an identity account to merge with the accounts selected in the Select Uncorrelated Accounts panel.

6. Click **Perform Merge** to perform the merge for these identities.
    The merge removes the accounts from the **Select Uncorrelated Accounts** table.

Chapter 24: Alerts

The Alerts page is used to view and define alerts. The alerts list is view-only; no action can be taken on alerts that have occurred within your system or the actions that those alerts initiated.

The Alert Definitions tab is used to manage alert definitions. Depending on your access, you can define, delete, edit, and enable or disable alerts. Under the Alert Definition tab, you can also set a Match Rule to either notify a user or to initiate a workflow or certification. You can set the Owner of the alert along with the Action Type under the Behavior section.

For detailed information, refer to the *IdentityIQ System Adminstration Guide* located in your `IdentityIQ_InstallationDirectory\doc\pdf` directory.

IdentitiyIQ User Guide

Chapter 25: Tasks

Task are used to automate the processes which build, update, and maintain the information contained within IdentityIQ. Use the basic tasks that SailPoint provides, or create and customize the task to meet the needs of your organization.

For detailed information, refer to the *IdentityIQ System Adminstration Guide* located in your `IdentityIQ_InstallationDirectory\doc\pdf` directory.

Chapter 26: Advanced Analytics

Advanced analytics enable you to create specific queries based on numerous aspects of IdentityIQ. These searches can be used to determine specific areas of risk and create interesting populations of identities.

Search results can be saved for reuse or saved as reports. In some cases, you can save your results as interesting populations of identities. When you save a search as a report, you can schedule the search on an continuous basis for monitoring and tracking purposes. When you save the search criteria as a population, you can use activity monitoring and statistical reporting of identities that fit that criteria in the same way that you use them for groups.

You can access the search page from the navigation menu bar. Go to **Intelligence -> Advanced Analytics**. Select a **Search Type** from the drop-down menu and enter the search criteria.

IdentityIQ advanced analytics is made up of the following search types:

- "Identity Search" on page 145. — generate searches on specific attributes of the users in your enterprise.
- "Advanced Identity Search" on page 150 — generate ad-hoc searches using boolean operations.
- "Access Review Search" on page 152 — generate searches based on certification criteria.
- "Role Search" on page 155 — generate searches on the roles in your enterprise.
- "Entitlement Search" on page 159 — generate searches on entitlements in your enterprise.
- "Activity Search" on page 161 — generate searches on activity over specific time periods and on specific applications, identities, groups, populations or targets.
- "Audit Search" on page 163 — generate searches for audit records for specific time periods and for specific actions, sources, and targets.
- "Process Metrics Search" on page 166 — generates searches based on business process metrics criteria.
- "Access Requests Search" on page 169 — generates searches for current and archived access requests.
- "Syslog Search" on page 166 — generates searches for specific technical support related information that relates to your IdentityIQ installation.
- "Account Search" on page 172— generates searches based on the accounts in your enterprise. These searches can find accounts by application, display name, owner, native identity, instance or any combination of these criteria.

Identity Search

Use the Identity Search page to generate searches on specific attributes of the identities in your enterprise. You can use these searches to determine specific risk areas or to define interesting populations of people from multiple organizations, departments and locations.

Search results can be saved for reuse or saved as reports. In some cases, you can save your results as populations of identities.

- When you save a search as a report, you can schedule the search on an continuous basis for monitoring and tracking purposes.
- When you save the search criteria as a population, you can use activity monitoring and statistical reporting of identities that fit that criteria in the same way that you use them for groups.

See also, "Group and Population User Interface" on page 99.

Identity Search Criteria

The Search Criteria panel is divided into four primary sections:

- "Saved Searches" on page 146 (not shown if no searches are saved)
- "Identity Attributes" on page 147
- "Entitlements" on page 148
- "Multi Valued Attributes" on page 149
- "Risk Attributes" on page 149

Search Criteria

The search criteria text fields support partial text strings using a starts-with protocol. For example, if you input "ro" in the Last Name field, the search results include Thomas Rowen and Betty Roberts.

Your use search criteria is used to narrow the search results. If you do not type information in a search criteria field, all possible choices are included. For example, if you do not select an application from the **Applications** list, all applications are included.

> **Note:** If the Load Saved Search panel displays, the search criteria for that search is loaded on the page. To create a new search click Clear Search.

Search Fields to Display

Use the Fields to Display panel on the right to select the identity and risk fields to display on the search results page.

The search fields are inclusive or AND type searches. Only actions matching values specified in all fields are included in the search results. For example, if you search by **First Name** John and **Last Name** Doe, the search results include only users with the character string John in their first name and Doe in their last name.

Advanced Searches

Use the Advanced Identity Search to create detailed, multi-layered filters to identify specific populations of users in your enterprise. To create complex queries into your identity cubes, you can create multiple filters and then group and layer them using And \ Or operations.

To display the advance search panel, click **Advanced Search** at the top left of the page. See "Advanced Identity Search" on page 150.

Saved Searches

When a previous search is saved to use later, the Saved Searches section displays at the top of the page. A saved search has the following information:

Table 1— Saved Searches Panel Descriptions

Field	Description
Saved Searches:	

Table 1— Saved Searches Panel Descriptions

Field	Description
Search Name	The names of past searches that you saved to reuse at a later time. To view the search results page, click the name of the saved search to view the search results page. **Note: These Saved Searches are only available for your use. To make identity searches available to users with Report access, save the search as a report.**
Loaded Saved Search:	
The name and description of your current saved query.	

Identity Attributes

Table 2— Identity Attributes Panel Descriptions

Criteria	Description
Identity Attributes Identity attributes are pulled from the identity mapping information that is set during deployment and configuration. **Note: You can use full names or partial strings in the text fields. For example, "ro" in the Last Name field returns Roberts and Brown.**	
Searchable Attributes Searchable Attributes are attributes you created and that are designated as Searchable when an identity is generated during deployment and configuration. For example, Department, Organization or Location.	
Last Name	Last name criteria to use in the query.
First Name	First name criteria to use in the query.
User Name	User name criteria to use in the query.
Display Name	The identity name in IdentityIQ.
Email	Email address criteria to use in the query.
Manager	Manager criteria to use in the query. The Identity search results include all users that report to managers that match the criteria in this field.
Is Inactive	Select **True** to include identities currently marked inactive or **False** to include identities that are currently active in the search results.
Is Manager	Select **True** to include identities that are marked as manager or **False** to include identities that are not marked as manager in the search results.
Type	Employee type: - Employee - Contractor - External Partner - RPA/Bots - Service Accounts
Software Version	**Only applicable to RPA/Bots** Software version associated with the Robotic Process Automation (RPA) /bots.

Table 2— Identity Attributes Panel Descriptions

Criteria	Description
Administrator	**Only applicable to RPA/Bots** The administrator of the Robotic Process Automation (RPA) /bots.
Applications	Select the applications to include in the search. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications or type a few letters in the field to display a list of applications that begin with that letter string. Identities need to match only one of the selected items to be included in the search results
Detected Roles	Select the detected roles to include in the search. If no roles are specified, all roles are included. Click the arrow to the right of the suggestion field to display a list of all roles or type a few letters in the field to display a list of roles that begin with that letter string. For hierarchical roles, the identity is included in the search results with each role in the hierarchy not only the highest level role.
Instance	The attribute that uniquely identifies a specific subdivision of an application.
Assigned Roles	Select the assigned roles to include in the search. If no roles are specified, all roles are included. Click the arrow to the right of the suggestion field to display a list of all roles or type a few letters in the field to display a list of roles that begin with that letter string. For hierarchical roles, the identity is included in the search results with each role in the hierarchy not only the highest level role.
Workgroup	Select the workgroups to include in the search. If no workgroups are specified, all workgroups are included.
Include Assigned Role Hierarchy	Select to include roles that are inherited from the assigned roles you selected for your search.

Specify the search criteria and columns to display and click **Run Search** to display the search results. From the search results page you can review the results of your search and save the search.

Entitlements

Table 3—Entitlements Panel Descriptions

Criteria	Description
Entitlement Filters Select an application, attribute name and entitlement then click **Add** to filter by your selection.	
Entitlement Metadata Filter your search to include identities with entitlements meet specific IdentityIQ-related criteria.	
Certification	**Has uncertified entitlements** — Use the drop-down list and select True or False to specify search results that include identities that have uncertified entitlements. **Has entitlements pending certification** — Use the drop-down list and select True or False to specify search results that include identities that have entitlements with pending certifications.

Table 3—Entitlements Panel Descriptions

Criteria	Description
Request	**Has entitlements that were not requested** — Use the drop-down list and select True or False to specify search results include identities with entitlements that were not requested. **Has pending requests for entitlements** — Use the drop-down list and select True or False to specify search results that include identities that have entitlements with pending access requests.
Other	**Aggregation Status** — Specify if the search must include identities whose entitlements are associated with applications that are Connected or Disconnected for aggregation. **Is Assigned** — Use the drop-down list and select True or False to specify search results that include identities with entitlements were assigned and not detected.

Multi Valued Attributes

Table 4—Multi Valued Attributes Panel Descriptions

Criteria	Description
Multi Valued Attributes: By default, IdentityIQ does not come pre-configured with any multi valued attributes. Multi-valued attributes are created during deployment and configuration. To limit the search, add values associated with a multi-valued attribute.The search results include the member list for the selected values. Use the and/or operator to define the search criteria. For example, for multi-valued identity attributes you can search by cost center or projects that have multiple values on multiple applications. For multi-value account attributes you can use group membership for specific accounts such as payroll or strategy and planning.	
Certification Score	The sum of compensated risk scores associated with certifications.

Risk Attributes

Risk scores and compensating factors are defined when IdentityIQ is configured.

Table 5—Risk Attributes Panel Descriptions

Criteria	Description
Composite Score	The total composite risk score for the identity.
Role Score	The sum of the compensated risk scores of each role assigned to this identity. To determine the compensated role risk score, compensating factors are applied to the role base risk score.
Role Score (Base)	The sum of role base risk scores. This score does not account for the compensating factors defined for role risk scoring.
Entitlement Score	The sum of the compensated risk scores of each entitlement assigned to this identity. To determine the compensated role risk score, compensating factors are applied to the entitlement base risk score.

Table 5—Risk Attributes Panel Descriptions

Criteria	Description
Entitlement Score (Base)	The sum of entitlement base risk scores. This score does not account for the compensating factors defined for entitlement risk scoring.
Policy Score	The sum of compensated risk scores associated with policy violations as defined when IdentityIQ was configured. Policies do not affect identity risk scores until a violation occurs.
Certification Score	The sum of compensated risk scores associated with certifications.

Advanced Identity Search

To access the Advanced Identity Search panel, click **Advanced Search** at the top-left of the Identity Search panel.

You can use the Advanced Identity Search to create detailed, multi-layered filters to identify specific populations of users in your enterprise. To create complex queries into your identity cubes., you can create multiple filters and then group and layer them using the Search Type operations. For certification of at-risk identities, you can schedule identity certifications for selected identities from the Identity and Advanced Identity Search Results page.

This section has the following topics:

- "Saved Searches" on page 146 (not shown if no searches are saved)
- "Identity Attributes" on page 147
- "Entitlements" on page 148
- "Multi Valued Attributes" on page 149
- "Risk Attributes" on page 149

After you enter the search criteria, click **Run Search**. The search results display.

To return to Identity Search, click **Identity Search** at the top-left of the panel.

The Advance Identity Search has the following information:

Table 6—Advance Identity Search Criteria

Criteria	Description
Add A Filter:	
Field	A filter characteristic associated with the identity type for your search. The drop-down list has all of the categories available to filter identities.
Search Type	The qualifier associated with the attribute value. For example, "equals" or "is like." The choices in this drop-down list are based on the Field specified.
Value	The value of the attribute.
Ignore Case	Specifies if case must be a factor when you filter for the value specified.
Filter(s):	
Operations	The drop-down list that have the And/Or values that control the interaction of the filters included in the query. The drop-down list is not visible unless two or more filters are created.

Table 6—Advance Identity Search Criteria

Criteria	Description
Group Selected	Use this button to group multiple filters in the Filters list to create layers or sub-filters in the query
Ungroup Selected	Use this button to ungroup grouped filters to edit the query.
Remove Selected	Use this button to remove the selected filter or sub-filter. **Note: If you select grouped filters and click this button, all filters in the group are removed from the query. To remove one filter from a grouped bundle, you must first ungroup the filters.**
view/edit filter source	Open a text box that enables you to view and edit a string view of the query. If you type invalid query code the green check mark is replaced with a red exclamation point.
Fields to Display: Specify the information to display on the Identity Search Results page. Each field defines a column on the results table. See "Identity Search Results" on page 151. Click **Identity Fields** or **Risk Fields** to show the display fields associated with each field. **Note: You must select at least one field to display on the results page.**	
Identity Fields	The basic identity fields, such as First Name, Manager, and Email, indicate information that IdentityIQ discovers based on definitions set during configuration. Role indicates all roles assigned to the identity. Application indicates all applications that the identity can access.
Risk Fields	The risk scores you want to display on the Identity Search Result page.

Identity Search Results

The identity search results display a table with all of the identities that match the criteria specified in your search. The columns in the table are based on the **Identity Fields** and **Risk Fields** that were selected from the **Fields to Display** list on the Identity Search page. From the results you can export your search results to file and save the search criteria to use future use.

Click **Refine Search** to return to the search criteria page.

Schedule Certification

You can use **Schedule Certification** to schedule certifications for any or all listed identities. Identity certifications are sent to the managers of identities that warrant special attention. These additional certifications do not replace regularly scheduled certification requests.

Result Options

Use the **Result Options** drop-down list on the Identity Search Results page to do the following:

- **Save or Update Search** — save the search for your own use. A list of saved searches displays at the top of the search page every time you log in.
- **Save or Update Search As Report** — searches saved as reports are added to your list of reports and can be scheduled to run on a continuous basis.
- **Save Identities as Population** — save the search as an interesting population of identities to use in activity monitoring and statistical reporting in similar way groups are used.
- **Show Entitlements** — display the entitlement information for all of the identities included in the list. The entitlements are separated into tables based on applications. To display a list of all users who are assigned the entitlement, click a value in any of the tables.

   The Percent of Population column displays the number of identities assigned to the specified attribute value on the application. The search results are displayed as a percentage and are based on the identities that have an account on the application.

Export Searches

Use the buttons on the top of the table to export the search results to file for archiving and auditing purposes. You can export search results to a .pdf, Microsoft Excel, or ArcSight CEF Flat File format.

Access Review Search

Use the Access Review Search page to generate searches for access review records. These searches can find access reviews by certifier, identity to be certified, access review type, access review phase, completion percentage, significant dates, tags or any combination of that criteria.

Search results can be saved as reports to reuse at a later time. When you save a search as a report, you can schedule the search on a continuous basis for monitoring and tracking purposes. See "Reports" on page 185.

The search fields are inclusive or AND type searches. Only actions matching values specified in all fields are included in the search results.

To limit the search results, use search criteria. If you do not type information or make a selection in a search criteria field, all possible choices are included. For example, if you do not provide a type in the **Type** field, events with any action type are included.

After you enter the search criteria, click **Run Search**. The search results are displayed on this tab.

Access Review Search Criteria

The Access Review Search page has the following information:

Table 7—Access Review Search Criteria

Criteria	Description
Saved Searches:	

Table 7—Access Review Search Criteria

Criteria	Description
Search Name	The names of past searches that you saved to reuse at a later time. **Note: These Saved Searches are only available for your use. To make searches available to users with Report access, save the search as a report. See "Audit Search Results" on page 165.**
Loaded Saved Search:	
The name and description of the current saved query.	
Run Search	Run the search with the criteria displayed on the current page. **Note: If you have modified the criteria of the Loaded Saved Search, the modified criteria is used for the search.**
Unload the Loaded Saved Search and clear all query options.	Clear Search.
Delete Search	Delete the specified Loaded Saved Query.
Access Review Attributes:	
Name	The name that you assigned to the access review when the access review was created. The search results include all access reviews that meet a specific criteria. The search is case-insensitive. You can type the entire name or a portion of the name. For example, you can type "mycert" to include that specific name or you can type "m" to include all access reviews that begin with the letter "m."
Certifier	The identity or workgroup that is assigned the access review request. The search results include all access reviews assigned to the value specified. Click the arrow to the right of the suggestion field to display a list of all certifiers or type a few letters in the field to display a list of identities or workgroups that begin with that letter string.
Identity	An identity in access review requests. The search results include all access reviews that have the specified identity. Click the arrow to the right of the suggestion field to display a list of all identities or type a few letters in the field to display a list of identities that begin with that letter string.
Type	Select an access review type from the drop-down list. The access review type can display additional options to filter the search.
Phase	Select an access review phase to limit the search. Review phases include Active, Challenge, Remediation, End.
Percentage Complete	Limit the search results by a percentage complete. Type a percentage in the field to the right and set the operator, greater than or less than.
Tags	Tags are assigned when access reviews are scheduled. You can use tags to classify access reviews for search and report purposes. The drop-down list has all the tags assigned to access reviews that you can access.

Table 7—Access Review Search Criteria

Criteria	Description
Filter By: **The following fields are displayed based on the Type of access review selected in the Type field. If no type is specified these fields are not displayed.**	
Manager Attributes	Specify a manager to include in your search for access review requests. Click the arrow to the right of the suggestion field to display a list of all managers or type a few letters in the field to display a list of manager names that begin with that letter string.
Group	Select a group or population to include in the search for access review requests. Note: The search results include access reviews assigned to the group or population. To display the valid options., click the arrow to the right of the Group and Value fields.
Application Attributes	Specify an application to search for access review requests. Click the arrow to the right of the suggestion field to display a list of all applications or type a few letters in the field to display a list of application names that begin with that letter string.
Role Attributes	Specify a role to search for access review requests. Click the arrow to the right of the suggestion field to display a list of all roles or type a few letters in the field to display a list of role names that begin with that letter string.
Account Group Attributes	Specify an account group and application to search for access review requests. Click the arrow to the right of the suggestion field to display a list of all account groups or applications or type a few letters in the field to display a list of account groups or applications that begin with that letter string.
Filter By: Date	
Date Type	Select an access review state for the dates specified. Review states include Created, Expiration, Signed or Finished.
Start Date	Specify a date to begin this search. For example, if you selected a type of Create, the search results include any access reviews created on or after the specified date.
End Date	Specify a date to end this search. For example, if you selected a type of Create, the search results include any access reviews created on or before the specified date.
Filter By: Signed Status	
Status	Specify access reviews by Signed or Unsigned status. Use the drop-down list to select **True or False**.
E-Signed	Specify access reviews by Electronic Signature status. Use the drop-down list to select **True or False**.
Signed By	Specify access reviews by the identity who signed off.
Fields to Display:	

Table 7—Access Review Search Criteria

Criteria	Description
Fields to Display	Specify the information displayed on the Access Review Search Results page associated with this search. The fields displayed change based on the type specified. Each field defines a column on the results table. See "Access Review Search Results" on page 155. **Note: You must select at least one field to display on the results page.**

Access Review Search Results

The access review search results display a table with all of the access reviews that match the criteria specified in your search. The columns in the table are based on the **Fields to Display** list on the Certification Search tab. From the results panel you can export your search results to file and save the search criteria for future use.

Click **Refine Search** to return to the search criteria page.

Result Options

Use the drop-down list to save search criteria to use in future searches:

- **Save or Update Search** — save the search for your own use. A list of saved searches displays at the top of the search page every time you log in.
- **Save or Update Search As Report** — save the search as a report. Searches saved as reports are added to your list of reports and can be scheduled to run on a continuous basis. See "Reports" on page 185.

Export Searches

Use the buttons to export the search results to file for archiving and auditing purposes. You can export search results to a .pdf or .csv format.

Role Search

Use the Role Search page to generate searches based on the roles in your enterprise. These searches can find roles by name, owner, type, or status. You can also search for roles by the number of users to whom they are assigned, manually or through role assignment rules, the number of entitlements they contain, their risk score weight, their association to other roles, the last time they were assigned or certified, or any combination of that criteria.

For example, you can identify roles that were created but are not being used by searching for setting **Detected Total** and **Assigned Total** to less than one (1).

> Note: The Refresh Role Indexes task must have run at least once before a roles search will yield results.

Search results can be saved as reports to reuse at a later time. When you save a search as a report, you can schedule the search on an on-going basis for monitoring and tracking purposes. See "Reports" on page 185.

The search fields are inclusive or AND type searches. Only actions matching values specified in all fields are included in the search results.

To limit the search results, use search criteria. If you do not type information or make a selection in a search criteria field, all possible choices are included. For example, if you do not provide a type in the **Type** field, events with any action type are included.

After you enter the search criteria, click **Run Search**. The search results are displayed on this tab.

Role Search Criteria

The Role Search page has the following information:

Table 8—Role Search Criteria

Criteria	Description
Saved Searches:	
Search Name	The names of past searches that you have saved to reuse at a later time. **Note: These Saved Searches are only available for your use.**
Loaded Saved Search:	
The name and description of your current saved query.	
Run Search	Run the search with the criteria displayed on the current page. **Note: If you have modified the criteria of the Loaded Saved Search, the search used the modified criteria.**
Clear Search	Unload the Loaded Saved Search and clear all query options.
Delete Search	Delete the specified Loaded Saved Query.
Role Attributes:	
Name	Enter a role name to include in the search. Entering a string of characters returns all roles with that string in their name that your controlled scopes enable you to view. For example, if you enter admin the search results include information for the roles System Administrator, SysAdmin, and Administrative Assistant.
Display Name	Enter a display name to include in the search. Entering a string of characters returns all roles with that string in their display name that your controlled scopes enable you to view. For example, if you enter System Administrator the search results include information for the display name System Administrator.
Owner	Enter the role owner to include in the search. Click the arrow to the right of the suggestion field to display a list of all role owners, or enter a few letters in the field to display a list of role owners that start with that letter string.
Type	Select the role type to include in your search. For example, IT, Organizational, or Business. Role types are defined for your enterprise during the role modeling process.

Table 8—Role Search Criteria

Criteria	Description
Status	Select the Enabled/Disabled status of the roles to include in the search.
Classification	Classifications can identify roles as potentially allowing access to sensitive, protected, or otherwise significant data. Choose any classifications to include in the search.
Detected Total	Specify an upper or lower limit for the number of identities that have this role detected that should be included in the search results. Detected roles are roles that are automatically assigned to identities based on the entitlements to which they have access. For example, to search for roles that were not detected by any identity during correlation, select Less Than from the drop-down list and type **1** in the empty field. The search results include all roles that were not automatically assigned to at least one identity.
Assigned Total	Specify an upper or lower limit for the number of identities that have this role assigned that should be included in the search results. Assigned roles are roles that were manually assigned to an identity by a user with role assignment authority or through a role assignment rule. For example, to search for roles that were not assigned to any identity, select Less Than from the drop-down list and type **1** in the empty field. The search results include all roles that were not manually assigned to at least one identity.
Entitlement Total	Specify an upper or lower limit for the number of entitlement a role can have. For example, if you select Less Than and type **3**, the search results include roles that contain two (2), one (1), or zero (0) entitlements.
Risk Score Weight	Specify an upper or lower limit for risk score weight assigned to a role for it to be included in the search results. For example, you can specify a Greater Than value to search for high-risk roles, or you can specify a Less Than value to search for roles that were created with a risk score weight that is too low for their type. In the second example, if your enterprise has a policy that requires that all IT-type roles have a risk score weight of 100, you can select IT from the **Type** drop-down list, select Less Than from the **Risk Score Weight** drop-down list, and type 100 in the empty field to return all IT-type roles with a risk score weight less than 100.
Associated To Another Role	Include roles that are associated with at least one other role or roles that are NOT associated with any other role. **True** — include roles that are associated with at least one other role. **False** — include roles that are NOT associated with any other roles.
Effective Access	Limit the search to the specific effective access list. Effective Access is any indirect access that was granted through another object. For example a nested group, an unstructured target, or another role.

Table 8—Role Search Criteria

Criteria	Description
Filter By: Date	
Date Type	Select a state to associate with the specified dates: **Last Membership Certification** — the date when the last role membership certification was performed. **Last Composition Certification** — the date when the last role composition certification was performed. **Last Assigned** — the date when the role was last assigned to an identity.
Start Date	Specify a beginning date for this search. The search results include information pertaining to any action performed on or after the specified date.
End Date	Specify an end date for this search. The search results include information pertaining to any action performed on or before the specified date.
Fields to Display:	
Fields to Display	Specify the information displayed on the Role Search Results page associated with this search. Each field defines a column on the results table. See "Role Search Results" on page 158. **Note: You must select at least one field to display on the results page.**

Role Search Results

The role search results panel displays a table with all of the roles that match the criteria specified in your search. The columns in the table are based on the **Fields to Display** list on the Role Search page. From this panel you can export your search results to file and save the search criteria for future use.

Click **Refine Search** to return to the search criteria page.

Result Options

Use the drop-down list to save search criteria to use in future searches:

- **Save or Update Search** — save the search for your own use. A list of saved searches displays at the top of the search page every time you log in.
- **Save or Update Search As Report** — save the search as a report. Searches saved as reports are added to your list of reports and can be scheduled to run on a continuous basis. See "Reports" on page 185.

Export Searches

Use the buttons to export the search results to file for archiving and auditing purposes. You can export search results to a .pdf or .csv format.

Entitlement Search

Use the Entitlement Search page to generate searches based on the entitlements or application object types in your enterprise. These searches can find application objects by attribute, owner, value, application, type, target, rights, annotation or any combination of that criteria.

Search results can be saved as reports for reuse. When you save a search as a report, you can schedule the search on a continuous basis for monitoring and tracking purposes. See "Reports" on page 185.

Entitlement searches that are saved as identity searches are only available from the Identity Search page. If you save an entitlement search as an identity search, the filters are converted to work on identity pages. The new search results include the identities that are in associated with the application objects for the original search

The search fields are inclusive or AND type searches. Only actions matching values specified in all fields are included in the search results.

To limit the search results, use search criteria. If you do not type information or make a selection in a search criteria field, all possible choices are included. For example, if you do not provide a type in the **Type** field, all application object types are included.

After you enter the search criteria, click **Run Search**. The search results are displayed on this tab.

Entitlement Search Criteria

The Entitlement Search page has the following information:

Table 9—Entitlement Search Criteria

Criteria	Description
Saved Searches:	
Search Name	**Note: These Saved Searches are only available for your use.** The names of past searches that you saved to reuse at a later time.
Loaded Saved Search:	
The name and description of your current saved query.	
Run Search	**Note: If you have modified the criteria of the Loaded Saved Search, the modified criteria is used for the search.** Run the search with the criteria that is displayed on the current page.
Clear Search	Unload the Loaded Saved Search and clear all query options.
Delete Search	Delete the specified Loaded Saved Query.
Account Group Attributes:	
Attribute	Type the name of an attribute to include in the search.
Owner	Type the entitlement owner to include in the search. Click the arrow to the right of the suggestion field to display a list of all possible owners or type a few letters in the field to display a list of possible owners that begin with that letter string.

Criteria	Description
Value	The value assigned to the attribute on an application.
Application	Select the applications to include in the search for entitlements. If nothing is selected, all application are included.
Type	Select the application object type to include in the search. If no application is specified all application object types from all applications are included in this list. If no application object types are specified, all are included in the search.
Classification	Classifications can identify entitlements as potentially allowing access to sensitive, protected, or otherwise significant data. Choose any classifications to include in the search.
Effective Access	Limit the search to the specific effective access list. Effective Access is any indirect access that was granted through another object. For example a nested group, an unstructured target, or another role.
Target	The specific target on an application to include in the search. Use the target filter to narrow the search results based on a specific application.
Rights	The rights associated with an entitlement on the target attribute. For example, create, read, update, delete, execute.
Annotation	The annotation field is an open field that you can use to add information to help describe permissions.
Searchable Attributes: The extensible entitlement attributes marked as searchable in the entitlements catalog.	
Fields to Display:	
Fields to Display	Specify the information displayed on the Entitlement Search Results page associated with this search. Each field defines a column on the results table. See "Entitlement Search Results" on page 160. **Note: You must select at least one field to display on the results page.**

Entitlement Search Results

The entitlement search results display a table with all of the entitlements that match the criteria specified in your search. The columns in the table are based on the **Fields to Display** list on the Entitlement Search page. From the results panel you can export your search results to file and save the search criteria to future use.

Right-click an entitlement in the table edit, view a summary of the entitlement or display a dialog that has a list of the identities associated with that entitlement.

Click **Refine Search** to return to the search criteria page.

Result Options

Use the drop-down list to save search criteria for use in future searches:

- **Save or Update Search** — save the search for your own use. A list of saved searches displays at the top of the search page every time you log in.
- **Save Search as Identity Search** — save the search as and identity search. Searches that are saved as identity searches are only available from the Identity Search page. If you save an account group search as an identity search, the filters are converted to work on identity pages. The new search results include the identities that are associated with the entitlements from the original search.
- **Save or Update Search As Report**— save the search as a report. Searches saved as reports are added to your list of reports and can be scheduled to run on a continuous basis. See "Reports" on page 185.

Export Searches

Use the buttons to export the search results to file for archiving and auditing purposes. You can export search results to a .pdf or .csv format.

Activity Search

Use the Activity Search panel to generate searches for activity information on applications and targets, by specific identities and population, over specific time periods. These searches can determine risk areas and track activity on sensitive applications in your enterprise.

Search results can be saved as reports for reuse. When you save a search as a report, you can schedule the search on an on-going basis for monitoring and tracking purposes. See "Reports" on page 185.

The search fields are inclusive or AND type searches. Only actions matching values specified in all fields are included in the search results.

To limit the search results, use search criteria. If you do not enter information or make a selection in a search criteria field, all possible choices are included. For example, if you do not select an application from the **Applications** list, all application configured to work with IdentityIQ are included.

After you enter the search criteria, click **Run Search**. The search results are displayed on this tab.

Activity Search Criteria

The Activity Search tab has the following information:

Table 10—Activity Search Criteria

Criteria	Description
Saved Searches:	
Search Name	The names of past searches that you saved for reuse. **Note: These Saved Searches are only available for your use. To make searches available to IdentityIQ users with Report access, save the search as a report. See "Activity Search Results" on page 163.**
Loaded Saved Search:	

Table 10—Activity Search Criteria

Criteria	Description
The name and description of your current saved query.	
Run Search	Run the search with the criteria displayed on the current page. **Note: If you have modified the criteria of the Loaded Saved Search, the modified criteria is used for the search.**
Clear Search	Unload the Loaded Saved Search and clear all query options.
Delete Search	Delete the specified Loaded Saved Query.
Activity Attributes:	
Type of Time Span:	
Time Period	If you want to filter by **Time Period**, select one or more time periods from the list. The definition for each time period is specified when IdentityIQ is configured.
Date of Activity	If you want to filter by **Date of Activity**, type the start and end dates for the search. **Start Date** — include information on activity that occurred on or after this date in the search results. **End Date** — include information on activity that occurred on or before this date in the search results. You can type the date manually or click the "..." icon to select a date from the calendar.
Actions:	
Action	The action that was performed For example, login or create. Use the Shift and Ctrl keys to select multiple list items. Identities need to match only one of the selected items to be included in the search results.
Applications:	
Source Application	Select the applications to include in the search. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications or type a few letters in the field to display a list of applications that begin with that letter string. Identities need to match only one of the selected items to be included in the search results.
Type of Target:	
Category	If you want to filter by **Category**, select the category to search from the drop-down list. The **Category** drop-down has all of the activity target categories defined on the Activity Target Categories page. Activity Target Categories are groups of targets from one or more applications. The **Target** list has all of the targets included in the selected category. This field is read only.
Targets	If you want to filter by **Targets**, specify the target that was acted upon. For example, a machine name for a login or a file name for a create action.
Identities or Interesting Populations:	

Table 10—Activity Search Criteria

Criteria	Description
Identities	The name of the user or workgroup that requested the action. Entering the first letter or letters, of a name displays a selection list of users or workgroups with names that have that letter string or click the arrow to the right of the field to display all names.
Interesting Population	The population of identities to include in the search. The **Interesting Populations** drop-down list has the populations created based on the results of Identity Searches. The list has only the populations that you created or that their creator designated as public.
Activity Results:	
Result	The result of the action, **Failure** or **Success**.
Fields to Display:	
Activity Fields	Specify the information displayed on the Advanced Activity Search Results page. Each field defines a column on the results table. See "Activity Search Results" on page 163. **Note: You must select at least one field to display on the results page.**

Activity Search Results

The activity search results display a table that has all of the activity that matches the criteria specified in your search. The columns in the table are based on the **Fields to Display** list on the Activity Search page. From the results tab you can export your search results to file and save the search criteria for future use.

Click **Refine Search** to return to the search criteria page.

Result Options

Use the drop-down list to save search criteria to use in future searches:

- **Save or Update Search** — save the search for your own use. A list of saved searches displays at the top of the search page every time you log in.
- **Save or Update Search as Report** — searches saved as reports are added to your list of reports and can be scheduled to run on a continuous basis. See "Reports" on page 185.

Export Searches

Use the buttons to export the search results to file for archiving and auditing purposes. The search results can be exported to a .pdf or .csv format.

Audit Search

Use the Audit Search tab to generate searches for audit records for specific time periods and for specific actions, sources, and targets. These searches can find and track events. The information included in the audit logs is different than application activity because the events in the audit log are not associated with an application or data source and may not be associated with a specific identity.

Before the audit logs collect any data to use in an audit search, IdentityIQ must be configured for auditing. Because collecting and storing event information in the audit logs can impact performance, a system administrator must specify the general actions and class actions to audit.

Search results can be saved as reports to reuse at a later time. When you save a search as a report, you can schedule the search on an on-going basis for monitoring and tracking purposes. See "Reports" on page 185.

The search fields are inclusive or AND type searches. Only actions matching values specified in all fields are included in the search results.

To limit the search results, use search criteria. If you do not type information or make a selection in a search criteria field, all possible choices are included. For example, if you do not provide a type in the **Type** field, events with any action type are included.

After you enter the search criteria, click **Run Search**. The search results are displayed on this tab.

Audit Search Criteria

The Audit Search tab has the following information:

Table 11—Audit Search Criteria

Criteria	Description
Saved Searches:	
Search Name	The names of past searches that you saved to reuse at a later time.
	Note: These Saved Searches are only available for your use. To make searches available to users with Report access, save the search as a report. See "Audit Search Results" on page 165.
Loaded Saved Search:	
The name and description of your current saved query.	
Run Search	Run the search with the criteria displayed on the current page.
	Note: If you have modified the criteria of the Loaded Saved Search, the modified criteria is used for the search.
Clear Search	Unload the Loaded Saved Search and clear all query options.
Delete Search	Delete the specified Loaded Saved Query.
Audit Attributes:	
Action	The action that was performed, for example, login, delete or signoff.
Source	The string that identifies the source of the event. The source is generally the name of an Identity object. The source can also be a less specific name such as, "scheduler" or "system." When the event occurs during an interactive session with the IdentityIQ Web application, identity names are used. When background tasks or anonymous requests are not run for a specific identity, abstract names are used.
Application	Type manually or use the drop-down list to select an audited application.
Instance	Type manually or use the drop-down list to select an instance of a specified audited application.
Attribute Name	Type manually or use the drop-down list to select an audited attribute name.

Table 11—Audit Search Criteria

Criteria	Description
Attribute Value	Type manually or use the drop-down list to select a value of a specific audited attribute.
Target	The object that was acted upon. For example, a machine name for a login or a file name for a create action.
Account Name	Type manually or use the drop-down list to select an audited account name.
Filter by Date	
Start Date	Include information on events that occurred on or after this date in the search results. You can type the date manually or click the **"…"** icon to select a date from the calendar.
End Date	Include information on events that occurred on or before this date in the search results. You can type the date manually or click the **"…"** icon to select a date from the calendar.
Fields to Display	Specify the information displayed on the Audit Search Results page associated with this search. Each field defines a column on the results table. See "Audit Search Results" on page 165. **Note: You must select at least one field to display on the results page.**

Audit Search Results

The audit search results display a table with all of the audit log information that matches the criteria specified in your search. The columns in the table are based on the **Fields to Display** list on the Audit Search page. There are also four (4) generic string fields that can be used to store additional information such as unstructured text messages or structured name/value pairs. From the results you can export your search results to file and save the search criteria for future use.

Click **Refine Search** to return to the search criteria page.

Result Options

Use the drop-down list to save search criteria to use in future searches:

- **Save or Update Search** — save the search for your own use. A list of saved searches displays at the top of the search page every time you log in.
- **Save or Update Search As Report**— save the search as a report. Searches saved as reports are added to your list of reports and can be scheduled to run on a continuous basis. See "Reports" on page 185.

Export Searches

Use the buttons to export the search results to file for archiving and auditing purposes. You can export search results to a .pdf, Microsoft Excel, or ArcSight CEF Flat File format.

Process Metrics Search

Use the Process Metrics Search page to generate searches on the business process metrics in your enterprise. These searches provide visibility to the detailed metrics that monitored processes and process steps generate. These searches help administrators create, manage, and monitor the identity business processes in IdentityIQ.

For example, you can determine the amount of time to run a defined business process and identity failures in the monitored steps of that process.

Search results can be saved as reports to reuse at a later time. When you save a search as a report, you can schedule the search on a continuous basis for monitoring and tracking purposes. See "Reports" on page 185.

The search fields are inclusive or AND type searches. Only actions matching values specified in all fields are included in the search results.

To limit the search results, use search criteria. If you do not type information or make a selection in a search criteria field, all possible choices are included. For example, if you do not provide a type in the **Type** field, events with any action type are included.

After you enter the search criteria, click **Run Search**. The search results are displayed on this tab.

Process Metrics Search Criteria

The Process Metrics Search page has the following information:

Table 12—Process Metrics Search Criteria

Criteria	Description
Name	Type the name or select a business process from the drop-down list.
Participants	Select one or more participants to include in your search.
Result Status	Select All, Success or Fail from the drop-down list.
Filter by Active Dates	Include a start or end date to limit your search results. Click the Start Date check box and select a date. Click the End Date check box and select a date.
Filter by Execution Time	Use one of the following filtering methods to limit your search results based on the process run times: **Average or Maximum —** Select Average or Maximum to display the average or maximum of all execution times. **Execution time greater than —** enter a minimum time unit as a baseline to start your search. **Time Unit —** select from minutes, hours or days

When you have finished entering search criteria, click **Run Search**. The search results are displayed on this tab.

Process Metrics Search Results

The Process Metrics Search Results panel displays the results based on your process metrics search criteria and includes the total number of execution attempts per process. To change the time units to minutes, hours or days, use the drop-down list at the top of the panel.

Click a row in the Process Metrics Search Results panel to display the Process Details sub-menu for a more detailed analysis of each process execution and select from the following options:

- View Executions — "Executions Panel" on page 167.
- View Step Overview — "Step Overview Panel" on page 167.

Executions Panel

To access the Executions panel, right-click on a row in the Results. The Executions panel displays information about the processes on specific identities.

> Note: **If the same process is run on an identity more than one time in the specified time frame, multiple listings of the execution displays.**

Table 13—Executions Panel

Name	Description
Execution Name	The name of the identity for whom the process was run. Click the execution name to view the Step Details Panel on page 167.
Started By	The name of the person who launched the process
Start Date	The date the process started.
End Date	The date the process completed.
Execution Time	The total amount of time for the process to complete. To change the time units to minutes, hours or days, use the drop-down list at the top of the panel.

Step Details Panel

The Step Details panel displays information about the transitions or steps for processes on specific identities.

Table 14—Executions Panel

Name	Description
Step or Approval Name	The name of the step or approval for the process.
Participant	The name of the person involved with the step.
Start Date	The date the step started.
End Date	The date the step completed.
Execution Time	The total amount of time for the step to complete. To change the time units to minutes, hours or days, use the drop-down list at the top of the panel.

Step Overview Panel

The Step Overview panel displays information about the steps or transitions for the processes.

Table 15—Step Overview Panel

Name	Description
Step Name	The name of the step or transition in the process. Click the step name to view the Step Information sub-menu and select from the following options: **View Participants** — Click to view the Participants panel. **View Approval Overview** — Click to view the Approval Overview panel.
Average Execution Time	Displays the average amount of time, from Start to Stop, for the step or transition.
Minimum Execution Time	Displays the least amount of time, from Start to Stop for the step or transition,
Maximum Execution Time	Displays the longest amount of time, from Start to Stop for the step or transition.
Number of Executions	Displays total number of executions attempts for the step or transition.

Participants

The Participants panel displays information about the identities in the steps or transitions for the processes.

Table 16—Participants Panel

Name	Description
Participant	The name of the identity in the step or transition of the process execution.
Approval Name	The name of the defined approval step.
Start Date	The date the step or transition started.
End Date	The date the step or transition completed.
Execution Time	The total amount of time or the step or transition to complete. To change the time units to minutes, hours or days, use the drop-down list at the top of the panel.

Approval Overview

The Approval Overview panel displays information about the approvals used in the step or transition for the processes.

Table 17—Approval Overview Panel

Name	Description
Approval Name	The name of the defined approval step.
Average Execution Time	Displays the average amount of time, from Start to Stop, for the approval step.
Minimum Execution Time	Displays the least amount of time, from Start to Stop for the approval step.
Maximum Execution Time	Displays the longest amount of time, from Start to Stop for the approval step.

Table 17—Approval Overview Panel

Name	Description
Number of Executions	Displays total number of executions attempts for the approval step.

Access Requests Search

Use the Access Requests Search page to generate searches on specific attributes of the access requests made in your enterprise.

Search results can be saved as reports to reuse at a later time. When you save a search as a report, you can schedule the search on a continuous basis for monitoring and tracking purposes. See "Reports" on page 185.

Any previously saved Access Request searches display in the Saved Searches section at the top of the page table to reuse at a later time.

After you enter the search criteria, click **Run Search**. The search results are displayed on this tab.

Access Requests Search Criteria

The Access Request Search page has the following information:

Table 18— Advanced Analytics - Access Request Search Page

Criteria	Description
Saved Searches:	
Search Name	The names of past searches that you saved to reuse at a later time. **Note: These Saved Searches are only available for your use. To make identity searches available to users with Report access, save the search as a report.**
Loaded Search:	
Run Search	Run the search with the criteria displayed on the current page. **Note: If you modify the criteria of the Loaded Saved Search, the modified criteria is used for the search.**
Clear Search	Unload the Loaded Saved Search and clear all query options.
Delete Search	Delete the specified Loaded Saved Query.
Access Request Attributes:	
Access Request ID	Identification number designated for individual requests.
Requestor	Name of the identity that made the request.
Requestee	Name of the identity for who made the request
Is Verified	Attribute was verified through the provisioning process.
Application	The application that is part of the access request.
Instance	The instance of the application that is part of the access request.

Criteria	Description
Operation	Type of operator used to fulfill request. For example, Add is an operation used in Request Roles and Lock is an action of a Certification.
Completion Status	The current state of a completed access request.
Priority	The priority assigned to the access request.
Request Type	The type of business process associated with the access request.
Approval State	The current state of the access request in the Approval phase.
Provisioning State	The current state of the access request in the Provisioning phase.
Reason	Indicates if an item was added (expanded) or filtered from the original request. For example, a role requires an entitlement or an entitlement requires and account. The compilation process adds or removes any required items in the provisioning process.
State	The current state of the access request.
Filter by: Date	
Request Date	Use the drop-down list to select from Request Date, Completion Date or Verified Date and select a Start Date and End Date.
Fields to Display	Select the columns to display in your search results.

Access Requests Search Results

The access requests search results display a table with all of the access request information that matches the criteria specified in your search. The columns in the table are based on the **Fields to Display** list on the Access Requests Search page. There are also generic string fields that can be used to store additional information such as unstructured text messages or structured name/value pairs. From the results you can export your search results to file and save the search criteria for future use.

Click **Refine Search** to return to the search criteria page.

Result Options

Use the drop-down list to save search criteria to use in future searches:
- **Save or Update Search** — save the search for your own use. A list of saved searches displays at the top of the search page every time you log in.
- **Save or Update Search As Report** — save the search as a report. Searches saved as reports are added to your list of reports and can be scheduled to run on a continuous basis. See "Reports" on page 185.

Export Searches

Use the buttons to export the search results to file for archiving and auditing purposes. You can export search results to a .pdf or .csv format.

Syslog Search

Use the Syslog Search page to generate searches on specific technical support information that relates to your IdentityIQ installation.

> **Note:** **This tab is used primarily to determine specific support information that SailPoint IdentityIQ support engineers can use for troubleshooting issues.**

Search results can be saved as reports to reuse at a later time. When you save a search as a report, you can schedule the search on a continuing basis for monitoring and tracking purposes. See "Reports" on page 185.

After you enter the search criteria, click **Run Search**. The search results are displayed on this tab.

Syslog Search Criteria

The Syslog Search page has the following information:

Table 19— Advanced Analytics - Syslog Search Criteria

Criteria	Description
Current Search:	
Run Search	Run the search with the criteria displayed on the current page.
Clear Search	Clear all query options.
Syslog Attributes:	
Incident Code	The ID associated with the logged exception. If the exception can be viewed in the UI, the ID is at the end of the message. The Incident Code assists help desk personnel to locate the exact exception.
Server	Name of the server running the code where exception was encountered. This information is helpful in clustered environments.
Level	Indicates the level of the logged exception. SailPoint supports logging WARN, ERROR and FATAL to the IdentityIQ database. Lower levels are logged using log4j if configured, but are not saved to the Syslog table in the database.
Username	User who was performing the action when the exception was encountered and logged. The username can be an individual user or a system.
Classname	Class in which the exception was encountered.
Message	The message included in the exception.
Line	The line of code executed when exception occurred.
Thread Name	The thread of code executed when the exception was encountered.
Filter by Date	
Start Date	Include information on events that occurred on or after this date in the search results. You can type the date manually or click the **"..."** icon to select a date from the calendar.
End Date	Include information on events that occurred on or before this date in the search results. You can type the date manually or click the **"..."** icon to select a date from the calendar.

Criteria	Description
Fields to Display Specify the information displayed on the Syslog Search Results page associated with this search. Each field defines a column on the results table. See Syslog Search Results on page 172. **Note: You must select at least one field to display on the results page.**	

Specify your search criteria and columns to display and click **Run Search** to display the search results.

Syslog Search Results

The Syslog search results display a table containing all of the access requests that match the criteria specified in your search. The columns in the table are based on the selections from the **Fields to Display** list on the Syslog Search page. You can export your search results to a file.

Click a line item on the Syslog Search Results page to view the full stack trace, if available.

Click **Refine Search** to return to the Syslog Search Criteria page.

Export Results

Use the export button to export the search results to file for archiving and auditing purposes. You can export search results to a .csv or ArcSight CEF Flat File format.

Account Search

Use the Account Search page to generate searches based on the accounts in your enterprise. These searches can find accounts by application, display name, owner, native identity, instance or any combination of these criteria.Search results can be saved as reports to reuse at a later time. When you save a search as a report, you can schedule the search on a continuous basis for monitoring and tracking purposes. See "Reports" on page 185.The search fields are inclusive or AND type searches. Only actions matching values specified in all fields are included in the search results.To limit the search results, use search criteria. If you do not type information or make a selection in a search criteria field, all possible choices are included. For example, if you do not provide an application in the Application field, all application's accounts are included.After you enter the search criteria, click Run Search. The search results are displayed on this tab.

Account Search Criteria

The Account Search page has the following information:

Criteria	Description
Saved Searches:	

Table 20— Advanced Analytics - Account Search Criteria

Criteria	Description
Search Name	The name of the past searches that you saved to reuse at a later time.
	These saved searches are only available for your use.
Loaded Saved Search:	
The name and description of your current saved query.	
Run Search	Run the search with the criteria that is displayed on the current page.
	If you have modified the criteria of the Loaded Saved Search, the modified criteria are used for the search.
Clear Search	Unload the Loaded Saved Search and clear all query options.
Delete Search	Delete the specified Loaded Saved Query.
Account Attributes:	
Application	Select the application to include in the search for accounts.
Display Name	Enter the Display name of account to include in the search.
Owner	If you want to filter by owner, select the owner to search from the drop-down list.
Native Identity	Select the native identity to include in the search for accounts.
Instance	Select the instance to include in the search for accounts.
Fields to Display	
Specify the information displayed on the Account Search Results page associated with this search. Each field defines a column on the results table. See "Account Search Results" on page 173.	
You must select at least one field to display on the results page.	

Account Search Results

The Account search results display a table containing all of the access requests that match the criteria specified in your search. The columns in the table are based on the selections from the Fields to Display list on the Accounts Search page. You can export your search results to a file.

Click Refine Search to return to the Account Search Criteria page.

Result Options

Use the drop-down list to save search criteria to use in future searches:

- Save or Update Search — save the search for your own use. A list of saved searches displays at the top of the search page every time you log in.
- Save or Update Search As Report — save the search as a report. Searches saved as reports are added to your list of reports and can be scheduled to run on a continuous basis.

See "Reports" on page 185

Export Results

Use the export button to export the search results to file for archiving and auditing purposes. You can export search results to a Microsoft Excel, .pdf or ArcSight CEF Flat File format.

Chapter 27: Manage Work Items

Use the Manage Work Items page to view all work items that are assigned to you or to a workgroup of which you are a member and to view all work items assigned by you. A work item is anything that requires a user to take an action before it is completed. Work items can be entire processes, such as certifications. Work items also include any part of a process, such as the approval of one entitlement for one user on one application.

The following tabs are available on the Manager Work Items page:

- "Work Items" on page 175
- "Work Item Archive" on page 176

Work Items

Use this page to view the work items assigned to you. The number displayed in the circle next to the access review title indicates the number of work items you have. This page contains a description of the work item along with the following information:

Table 1—Work Item Page Listings Descriptions

Item	Description
Type	The type of the work item, for example Approval, Access Review, or Policy Violation.
Description	The work item description. For longer descriptions, click **Read More** to see the full text
Created	The creation date
Work Item ID	The specific ID assigned to the work item
Owner	The work item owner
Requester	The identity that made the request for the specific work item

Display Options

Display options for this page include:

- Sort by — Select this option to display access reviews by items such as, Type, Requester, or Priority.
- Sort order icon — Reverse the sort order
- Filter — Use filters to define a specific set of work items
- Search — Search for a specific work item
- Show — Select the number of items to display per page

Features

You can perform the following actions from the Work Item page:

> Note: **The Administrator must enable the option to Allow priority editing on work items before that option is available.**

- Information — Click the Information icon to display the Details panel containing the Work Items Details, Identity Details, and Forwarding History.

- Forward — Click the Forward icon to forward a work item to a different IdentityIQ user or workgroup. When you forward a work item, it is removed from your list and does not reflect in your risk score statistics. Owner history and all comments are maintained with the work item.

- View — Click **View** to display the work item detail page and complete the work item. The page displayed is dependent on the work item type.

- Edit Priority — Click the priority (flag) icon and select a different priority.

Work Item Archive

Use the Work Item Archive page to view work items that were completed. Only work item types that are configured as archivable are displayed on this page.

Click the drop-down list to specify which of the following work items to display.

To customize the information displayed in the Work Item Archive table, mouse over one of the header rows, click the drop-down arrow to reveal the sub-menu and select the desired columns from the Columns pop-out menu.

Use the **Filter** and **Advanced Search** options to narrow the work items listed.

Click a line item to display detailed information about the work item.

The Manager Work Items table includes the following types of work items:

Table 2—Work Item Archive Column Descriptions

Column Name	Description
ID	Identification number assigned to the work item.
Name	The name of the work item.
Type	The type of work item.
Requester	The name of the user that assigned this work item to you.
Workgroup	Displays the workgroup to which this work item is assigned, if applicable.
Owner	The name of the identity who has purview over the work item.
Completed By	The name of the identity that completed the work item.
Created	The date the work item was assigned.
Modified	The date on which the work item was last modified.
Archive	The date on which the work item was archived.
Priority	Specifies the priority level to which the work item was designated. Use the drop-down list and edit the priority level. This edit is visible in the Work Items Manager.
Access Request ID	Identification number designated for the Lifecycle Manager access request.

Chapter 28: Policy Violations

Policies in IdentityIQ check identities for certain conditions that are unwanted, or even considered dangerous - for example, a set of roles that should not be combined in a single identity (such as "payment preparation" and "payment approval"), two conflicting values of a multi-valued attribute, a high risk score, or even cross-application combinations of permissions.

Policy violations occur when an identity is found to be in violation of an active policy.

The Policy Violations page shows you any policy violations you are responsible for acting on. You can revoke the problematic access, allow the violation to continue for a set period of time, or take other actions such as forwarding the violation to another user.

Use the Policy Violations page to manage policy violations outside of certifications. This page enables you to identify policy violations as soon as they are detected, and take immediate action to resolve those violations.

Overview of the Policy Violations Page

The Policy Violations page lists policy violations that are marked as active and violations owned by you or one of the workgroups to which you belong. When a policy is defined, an owner to a policy violation can be defined. The policy violation owner is a chosen identity, manager of the person who violated the policy, or an identity created by running a rule. You cannot take action on your own violations.

Based on how your system is configured the Policy Violations page can have the following tabs and actions:

> Note: The number on the tab indicates the number of items listed on the associated tab page.

- **Open** Tab - From this tab you can:

    - **Allow** or **Revoke** a violation.

    - Make **Bulk Decisions** on multiple violations.

    - View **Details** about a violation from the menu icon for the violation.

    - Launch a certification of items, using the **Certify** option (in the **Bulk Decisions** menu)
- **Complete** Tab - From this tab you can

    - Launch a certification of items, using the **Certify** button

    - **Edit Decision** from the **3-line menu** icon for the violation.

    - **View Decision** for a revoked violation from the **3-line menu** icon .

    - View **Details** about a violation from the **3-line menu** icon for the violation.

For information on managing policy violations through work items, refer to the *IdentityIQ User Guide* .

Accessing the Policy Violations Page

Policy violation can be accessed from the menu bar using **MyWork > Policy Violations**. Depending on how your system is configured, you can also access the Policy Violations page from the QuickLinks menu > **My Tasks > Policy Violations** or from a Home page QuickLink card.

Most users will see the same list of policy violation from the menus and the QuickLinks card. Users with **System Administrator** or **Policy Administrator** capabilities will see different results based on how they access the page:

- The QuickLinks menu and card will show System Administrators and Policy Administrators o**nly the violations for which they are themselves are responsible**.

- The My Work > Policy Violations menu will show System Administrators and Policy Administrators **all policy violations in the system,** not just the ones they are responsible for.

Display Options

Use the **Filter** icon to limit what is displayed on the Policy Violations Page. You can filter violations by user name, (including first name and last name), policy type, status, and policy violation ID, using any combination of filters and values. To apply your filter criteria, click **Apply**.

When filtering is applied, the Filter button in the Policy Violations turns green, to alert you that you are seeing a filtered subset of all your items. To clear filtering, click **Filter** again, then click **Clear**.

You can sort the information in the table in ascending or descending order by clicking on any of the column headings.

Accessing Policy Violation Work Items

Depending on how the policy was configured, you can also view your policy violation items in your work item listing, by clicking **My Work > Work Items**. In the Work Items page, policy violations are listed along with any other work items you may have. You can filter, search, and sort the items in this list to limit what is shown.

In the Work Items Page, you can:

- Click the **Info** icon to see information about violation item

- Forward the violation item to another user to process, using the **Forward (arrow)** icon

- Click **View** to open a detailed view of the item. When you click **View**, you have additional options for managing the item:

  - **Add Comments** to the item

  - Click the **Go to violation link** to see options to Allow, Revoke/Correct, or Certify the item

  - Save any changes (such as the addition of a comment) you have made to the item

For more detailed information about the details and options in this page, see "Policy Violation Work Items" on page 182.

Policy Violations Open Tab

The Open tab lists policy violations awaiting your attention. The **Open** tab includes the following:

Table 1—Policy Violations Page: Open Tab Column Descriptions

Column	Description
Identity	First and last name of the user who is in violation of the policy
Policy Name	Name of policy that is violated.

Table 1—Policy Violations Page: Open Tab Column Descriptions

Column	Description
Rule	Specific rule in the policy that is in violation.
Owner	The person responsible for acting on the violation. If the creation of work items is enabled in the policy configuration, this is also the person who receives the work item triggered by the violation.
Description	Description of the violation from the Policy Configuration page.
Decisions	The available decisions you can make on this violation.
Details	Click the 3-line menu icon for the option to view details about the item.
Bulk Decisions	Depending on how the policy was configured, you may have the option to select multiple items and process them in bulk. The **Bulk Decisions** menu is also where the option to **Certify** the item is located.

Violation Decisions and Actions

Note: **You cannot take action on your own violations.**

Depending on how your system is configured the following decision options can be available:

Table 2—Policy Violations Page: Open Tab Decisions and Actions

Decision	Description
Allow	Select the **Allow** icon to open the **Allow Violations** dialog. When you allow, or mitigate, a violation you are setting a time period in which the identity is allowed to work in violation of the policy without affecting compliance or risk. The date field shows the end date of this period, when the violation will reappear in this list and in certifications. Whether or not you can edit the date field depends on how your system administrator has configured your system's Compliance Manager settings. Add any comments necessary to explain this mitigation decision.
Revoke	You cannot perform bulk violation corrections and only SOD violations can be corrected. Select the **Revoke** icon to display the detailed view of the violation and make a revocation decision based on the items displayed. You must revoke one complete set of offending roles or the violation remains. The Revocations can be done automatically, if your provisioning provider is configured for automatic revocation, by generating a help ticket, if your implementation is configured to work with a help desk solution, or manually using a work request assigned to a IdentityIQ user.
Delegate	This option is available only when the **Enable Line Item Delegation** option is enabled in your system's Compliance Manager global settings. Select **Delegate Violation** to display the delegate violation panel. Use the fields to associate a work item with the selected policy violations and assign it to the appropriate user for corrective action. The owner of a policy, or a compliance officer who is tracking violations, may not be the same person who can make the decision as to how to correct the violation. On the delegate violation panel, enter the full name of the person to whom you assigning this work item. Entering the first few letters of a name displays a pop-up menu of IdentityIQ users with names containing that letter string. You can also select a recipient from the **Manually Select Recipient** drop-down list. Enter a description and comments as needed to assist the recipient.
Bulk Decisions	Select multiple violations and use this option to take bulk actions, such as Allow and Certify.

Table 2—Policy Violations Page: Open Tab Decisions and Actions

Decision	Description
Certify	The **Certify** option is under the **Bulk Decisions** menu. Select items in your list, then click **Certify** to open the Schedule Certification page, to set up a certification. From this page you can schedule full certifications for the identities appearing on the policy violations list. You can use this option to provide another way to monitor identities that might be at risk within your enterprise.
Comments	If this option is enabled, you can add comments. In some instances, you may be *required* to add comments.
Details	Select this option to view detailed information.

The following reference table lists the available options for specific policy types:

Table 3—Policy Violations: Available Options by Policy

Policy Type	Available Policy Violation Options
Account	Allow, Certify
Advanced Entitlement Policy	Allow, Certify, Revoke
Advanced Policy	Allow, Certify
Entitlement Policy	Allow, Certify, Revoke
Activity Policy	Allow, Certify
Risk Policy	Allow, Certify
SOD Policy	Allow, Certify, Revoke

After you have made your decisions, click **Save**.

Policy Violations Complete Tab

The **Complete** tab lists the items you have made a decision on and saved. The **Complete** tab contains information about the Identity, Policy Name, Rule, Owner, Description, and Decisions for each policy violation in the list.

Based on how your system is configured, the **Complete** tab can include the following options:

Options	Description
Certify	You can select items in your list and click **Certify** to open the Schedule Certification page, to set up a certification. From this page you can schedule full certifications for the identities appearing on the policy violations list. You can use this option to provide another way to monitor identities that might be at risk within your enterprise.
Edit Decision	Click Edit to make changes to the decision
Details	Select this option to view detailed information.

Policy Violation Work Items

Policy violation work items can be assigned by policy reviewers from the Policy Violation page, or automatically by business processes, violation rules, or alerts configured in your enterprise. These work items are generated outside of the certification process. Policy violation work items can also be created when the Check Active Policies task detects active policy violations.

Approve Policy Violation work items created through a business process can appear and act differently than work items created manually or automatically through an alert or rule. Work items created through a business process are highly customizable, and allow you to take action on the policy violation directly from the work item, instead of having to go to the Policy Violations page. The actions that are enabled, and the resulting actions based on the selection made, depend upon how the business process was defined.

In the Work Items Page, you can:

- Click the **Info** icon to see information about violation item
- Forward the violation item to another user to process, using the **Forward (arrow)** icon
- Click **View** to open a detailed view of the item. When you click **View**, you see more information about the item, and have additional options for managing the item, as described in Table 5 :

Table 5—Policy Violation Work Item Description

Category	Description
Summary:	
Requester	The name of the person or workgroup that assigned the work item.
Owner	The name of the person who is responsible for this work item.
Description	A brief description of the action required for this work item.
Created	The creation date of this work item.
Expiration	The work item expiration date, if one applies. Default work item expiration dates can be set when IdentityIQ is configured.
Priority	The severity of the work item.
History	Any historical information attached to this work item.

Table 5—Policy Violation Work Item Description

Category	Description
Comments Button	
Comments	This section contains any comments that the requester of the work item or the assignee entered. When new comments are added, the requester and the assignee are notified. This notification provides a communication and tracking mechanism for this work item.
Address the following policy violation:	
Identity name	The user name or login ID of the identity that is in violation of the policy.
Policy	The policy type, Separation of Duty, Activity, Account, or Risk.
Policy Description	The description of the policy as entered when the policy was created.
Policy Violation Owner	The name of the person who owns this violation.
Rule	The name of the rule that caused the policy to be in violation.
Rule Description	The description of the rule that was broken.
Compensating Control	Any compensating controls associated the policy. For example, in some cases managers may be exempt for certain separation of duty policies.
Correction Advice	Any correction advice associated with the policy. This advice is added when the policy is created.
Score Weight	The risk score assigned to this violation. This score is used for identity risk score generation. **Note: Risk scores for policy violations are configured in the Risk Scoring Configuration feature, in Identities > Identity Risk Model**
Go to violation	A link to the policy violation page.
Policy Violation Page	
Summary	Details of the policy and the rule that caused the violation.
Violation Decision	Can include Allow, Revoke, and Certify. Only available on work items created by a business process. The action enabled by the business process used to create this work item.

The Policy Violation View Work Item page can have the following action buttons:

- **Forward** — Displays the Forward Work Item dialog enabling you to forward the work item to another user or workgroup.
  You can enter the first few letters of a name in the **Forward To** field to display a pop-up menu of IdentityIQ users and workgroups with names containing that letter string. Select a name from the list and add your comments.

- **Add Comment** — Inserts a comment about the work item or policy violation.
  When you add comments to work item, the requester of the work item is notified. This notification provides a communication and tracking mechanism for the work item because all comments are stored and displayed until the work item is complete.

- **Complete** — Displays a dialog where you can add comments prior to closing the work item and marking it as complete.

- **Back To Home** — Returns you to the Policy Violations list page. If you do not have access to that page, your IdentityIQ Home page is displayed.

Chapter 29: Reports

Use IdentityIQ reporting to collect the information you need to manage the compliance process. Reporting replaces manual searches for data located in various systems around your enterprise.

SailPoint provides a number of standard reports that can be run without changes. You can also use the standard reports to create custom reports that are specific to your needs.The provided reports are displayed on the Reports tab. The following types of report templates are provided:

- **Detailed Reports** — include key data about specific areas in IdentityIQ. The information can be presented in table or grid format. The results can be exported to a .csv file and used in spreadsheets.
- **Archived Reports** — include end-of-period and task information that is formatted for easy dissemination of key audit information. Due to the large amount of data that is generated, the best option is to export the report results to a .pdf file
- **Summary Report** —include end-of-period and task information that is formatted for easy dissemination of key audit information. Due to the large amount of data that is generated, the best option is to export the report results to a .pdf file

The Reports page has the following tabs:

- My Reports Tab — displays all of the reports that you created. See "My Reports Tab" on page 185.
- Reports Tab — view all reports created for your enterprise, or create new reports. See "Reports Tab" on page 186.
- Scheduled Reports Tab — view all reports scheduled to run.
- Report Results Tab — view the results of previous reports See "Report Results Tab" on page 186.

My Reports Tab

The My Reports tab displays all of the reports that you created using the templates, or standard reports, provided on the Reports tab. These reports are only available for your use. You can use scoping to make the results visible to other users.

Reports are listed by category.Use filtering to limit the number of reports displayed in the table. Enter a letter, or partial name in the **Search** field to display reports with names containing that letter pattern.

For a complete list of the report templates provided, see "Report List" on page 192.

Use this page to edit, run, schedule, export or delete your custom reports. Right-click the report name and select an option from the pop-up menu. When you select an export function, the report is run and the results are displayed in the selected format. For Detailed and Summary type reports the **Export to CSV** option is not available.

See "Working with Reports" on page 181.

To view a list of all scheduled reports, see "Scheduled Reports Tab" on page 179.

To view reports after they have completed, see "Report Results Tab" on page 186.

The My Reports tab has the following information:

Column	Description
Name	The name of the report as defined when the report was created.
Description	A brief description of the specific report.

Reports Tab

SailPoint provides a number of standard reports that can be run without changes or that can be used as templates to create custom reports. The provided reports are displayed on the Reports tab. Three types of report templates are provided and include, Detail, Archive, and Summary reports.

> **Note:** **You cannot write over the report templates on the Reports tab. If you edit a report template from Reports tab and save the changes, you must assign a name to the new report and it is added to the report list on the My Reports tab.**

Reports are listed by category. Use filtering to limit the number of reports displayed in the table. Enter a letter, or partial name in the **Search** field to display reports with names containing that letter pattern.

For a complete list of the report templates provided, see "Report List" on page 192.

Use this page to create, edit, run, schedule, export or delete your custom reports. Right-click the report name and select an option from the pop-up menu. When you select an export function, the report is run and the results are displayed in the selected format. For Detailed and Summary type reports the **Export to CSV** option is not available.

See "Working with Reports" on page 181.

To view a list of all scheduled reports, see "Scheduled Reports Tab" on page 179.

To view reports after they are completed, see "Report Results Tab" on page 186.

To create reports based on searches on identity, activity, and audit information, see "Identity Search" on page 145, "Activity Search" on page 161, and "Audit Search" on page 163.

The Reports page has the following information:

Table 2—Report Tab Descriptions

Column	Description
Name	The name of the report template.
Description	A brief description of the specific report.

Report Results Tab

The Report Results page displays a list of reports run in the IdentityIQ application to which you have access. If scoping is active you may only have access to reports in scopes that you control.

Use the filtering options to limit the number of reports displayed in the table. Entering a letter, or partial name, in the **Report Names** field displays any reports with names containing that letter pattern.

Table 3—Report Results Column Descriptions

Column	Description
Name	The name of the report.
Date Complete	The date and time stamp of when the report completed running.
Result	The result status, Pending, Successful, or Failed.
Signoff	The status of the sign off request for the report results. **None** — no sign off required **Waiting** — sign off request not complete **Signed** — a sign off decision has been made
Owner	The user that created the report.

Click a report name in the View Report Results table to display the Report Results page for that report. Each Report Results page displays information about the report as well as the information collected. Each report type includes information specific to the data collected.

See "Report List" on page 192 for details on the information returned by each report type.

If a report was scheduled to run but there were no results, navigate to the Scheduled Report page and ensure that errors did not occur when the report was run.

To delete report results, right-click the result and select **Delete**. Reports that require a sign off can only be deleted by a user with the Signoff Administrator capability.

Every report can be exported to an external file. Use the icons below the Details section to export the report results.

> Note: **Export report names are cropped at 31 characters.**

Working With Reports

The most common report tasks include the following items:

"How to Create a New Report" on page 188."How to Run a Report" on page 189"How to Edit a Report" on page 190"How to Schedule a Report" on page 191"How to Complete Report Work Items" on page 192Export Results

You can also select one of the export features to launch a report and export the results directly to an external file. Exported reports are not included in the list on the View Report Results page.

Report Work Items

Reports that require sign off generate work items and email notifications that are assigned to the designated signers. Sign off decisions are retained with the report results for tracking purposes.

New Reports

To create a new report, on the Reports tab, click an existing report or right-click and select **Save As New Report** display the New Report page.

Existing Reports

To edit an existing report on the My Reports tab, click a report name or right-click and select **Edit** to display the Edit Report page.

To edit reports based on searches on identity, see "Identity Search Results" on page 151.

To edit reports based on searches on identity, activity, and audit information, see "Identity Search Results" on page 151, "Activity Search Results" on page 163, and "Audit Search Results" on page 165.

Scheduled Reports

To schedule a report to run at a later time or on a recurring basis, right-click a report name and select **Schedule** from the drop-down list to display the New Schedule dialog. You can schedule reports to run once, hourly, daily, weekly, monthly, quarterly or annually to meet the requirements of your enterprise and auditors.

To delete a report, right-click the report name and select **Delete** from the drop-down menu. Click **Yes** on the confirmation pop-up to delete the report. When you delete a report from the Reports table, all associated report results are deleted as well.

How to Create a New Report

Use the New Report page to create reports for your organization based on the reports provided. Reports can be as general (all users in your organization) or specific (one user) as required.

See "Standard Report Properties" on page 193 for the complete list of reports provided with IdentityIQ.

Searches defined on the search pages can also be saved as reports. Reports created on the search pages are saved in the Search category on the My Reports tab.

Procedure

1. Access the Reports page from the navigation menu bar. Go to **Intelligence -> Reports**.

2. Right-click a report on the My Reports or Reports tab and select **Save As New Report**.

3. Enter a name and brief description of the new report.
   This information is displayed on the My Reports table when the new report is saved.

4. *Optional*: Require sign off.
   a. Activate Required sign off to expand the Signoff Properties section.
   b. Specify the required signers.
      Enter the first letter, or letters, of an identity to display a selection list of valid identities containing that letter string, or click the arrow to the right of the field to display a list of all users.
      You can add as many signers as required.
   c. Select an email notification template from the Initial Notification Email drop-down list. For example, the Report Result Signoff template.
      Templates are created and defined when the application is configured.
   d. Specify the escalation criteria for the sign off request.
      None — no reminder emails are sent and no escalation is performed for this work item.
      Send Reminders — email reminders are sent at the configured interval.
      Reminders then Escalation — the configured number of reminders are sent and then the work item is escalated to the signers manager.
      Escalation only — this work item is escalated after the configured interval with no reminders being sent.
      Escalation intervals are set when the application is configured.

5. Select a **Previous Result Action** from the drop-down list. **Rename Old** is select by default.
   Previous result actions determine how subsequent runs of this report react to existing report results.

   Delete — overwrite the previous report results with the new information.

   Rename Old — append a numeral to the name of the old report result and preserve both.

   Rename New — append a numeral to the name of the new report result and preserve both.

   Cancel — cancel the new run of the report.

6. *Optional*: Allow concurrency. Activate the **Allow Concurrency** check box to enable two identical reports to run at the same time.
   If enabled, allow concurreny appends a numeric value to the name of the report that started second.

   If disabled, the second report is canceled and an exception sent to the requestor.

7. *Optional*: Assign an email recipient to receive notification of report completion.
   Enter the first letter, or letters, of an identity to display a selection list of valid identities containing that letter string, or click the arrow to the right of the field to display a list of all users.

8. *Optional*: Enter the maximum number of results to display in the report results.

9. *Optional*: Enter a scope for the report results. Enter the first few letters of a scope name to display the select box, or click the arrow to the right of the field to display all of the scope you control.
   Only identities that control the assigned scope can view the results of a scoped report.

   If scope is active and you do not explicitly assign a scope, the results are given your assigned scope.

10. Specify the report options required for the report you are creating.
    Each report type displays unique report options. **See** "Report List" on page 192 **for details on each report type.**

11. Specify the information will display in the report results.

12. Click **Save** to save the new report to the My Reports table.
    — OR —

    Click Save and Execute to save the report to the My Reports table and run it immediately.
    The Report Results page displays when the report completes.

    — OR —

    Click Save and Preview to preview the report results.

    — OR —

    Click Execute to run without saving.

    See "Report Results Tab" on page 186.

How to Run a Report

Right-click the report name and select **Execute** or **Execute in background**. **Execute** displays a pop-up progress window and opens the Report Results page when it is complete. **Execute in background** launches the report in the background. To track progress or to view the finished report, navigate to the Report Results tab.

Procedure

1. Access the Reports page from the navigation menu bar. Go to **Intelligence -> Reports**.

2. Navigate to the My Reports tab to view a list of your saved reports.

3. Right-click a report and select **Execute** or **Execute in background**.
   Execute displays a pop-up progress window and opens the Report Results page when it is complete. **Execute in background** launches the report in the background.

4. To track progress or to view the finished report, navigate to the Report Results tab.

See "Report Results Tab" on page 186.

How to Edit a Report

Use the Edit Report page to make changes to an existing report.

Procedure

1. Access the Reports page from the navigation menu bar. Go to **Intelligence -> Reports**.

2. Navigate to the My Reports tab to view a list of your saved reports.

3. Click a report, or right-click a report and select **Edit** from the drop-down list to open the Edit Report page.

4. Edit the **Name** and **Description** section as needed.

5. Select a **Previous Result Action** from the drop-down list. **Rename Old** is select by default.
    Previous result actions determine how subsequent runs of this report react to existing report results.

    Delete — overwrite the previous report results with the new information.

    Rename Old — append a numeral to the name of the old report result and preserve both.

    Rename New — append a numeral to the name of the new report result and preserve both.

    Cancel — cancel the new run of the report if a report result with the same name exists.

6. *Optional*: Allow concurrency. Activate the **Allow Concurrency** check box to enable two identical reports to run at the same time.
    If enabled, allow concurreny appends a numeric value to the name of the report that started second.

    If disabled, the second report is canceled and an exception sent to the requestor.

7. *Optional*: Assign an email recipient to receive notification of report completion.
    Enter the first letter, or letters, of an identity to display a selection list of valid identities containing that letter string, or click the arrow to the right of the field to display a list of all users.

8. *Optional*: Require sign off.
    a. Activate Required sign off to expand the Signoff Properties section.
    b. Specify the required signers.
        Enter the first letter, or letters, of an identity to display a selection list of valid identities containing that letter string and select a signer.
    c. Click Add to List to add the identity to the signers list.
        You can add as many signers as are required.
    d. Select an email notification template from the Initial Notification Email drop-down list. For example, the Report Result Signoff template.
        Templates are created and defined when the application is configured.
    e. Specify the escalation criteria for the sign off request.
        None — no reminder emails are sent and no escalation is performed for this work item.
        Send Reminders — email reminders are sent at the configured interval.
        Reminders then Escalation — the configured number of reminders are sent and then the work item is escalated to the signers manager.
        Escalation only — this work item is escalated after the configured interval with no reminders being sent.
        Escalation intervals are set when the application is configured.

9. *Optional*: Enter the maximum number of results to display in the report results. This option is available on a limited number of reports.

10. *Optional*: Enter a scope for the report results. Enter the first few letters of a scope name to display the select box, or click the arrow to the right of the field to display all of the scope you control.
Only identities that control the assigned scope can view the results of a scoped report.

    If scope is active and you do not explicitly assign a scope, the results are given your assigned scope.

    See **"Report List" on page 192** for details on each report type.

11. Click **Save** to save the new report to the My Reports table.
    — OR —

    Click Save and Execute to save the report to the My Reports table and run it immediately.
    The Report Results page displays when the report completes.

    — OR —

    Click **Save and Preview** to preview the report results.

    — OR —

    Click **Execute** to run without saving.

    See **"Report Results Tab" on page 186**.

How to Schedule a Report

Use the Schedule Report dialog to schedule reports to run at slow processing times or on a recurring basis as need to maintain compliance in your enterprise.

The New Schedule dialog enables you to assign a unique name and description to the report being run at the schedule time. The unique schedule name and description display on the Report Results table so that a report run from the Reports page does not overwrite the scheduled report. For example, if you define and schedule a Weekly All Violations Report that you download and archive for auditing purposes, someone running the All Violations Report mid-week does not overwrite the information in your scheduled report.

Procedure

1. Access the Reports page from the navigation menu bar. Go to **Intelligence -> Reports**.

2. Right-click a report name on the My Reports or Reports tabs and select **Schedule** from the drop-down list to open the New Schedule dialog.

3. Enter a unique name and description for this schedule report.
   This is the name and description that display in the Report Results table and distinguish this scheduled version of the report from the same report executed from the reports tables. Defining a unique name on this page ensures that scheduled reports are not overwritten by mistake.

4. Enter the date and time to launch the first execution of this report.
   You can enter the date manually, or click the ... icon to select a date from the calendar.

   — OR —

   Select the **Run Now** field to run the report immediately after clicking **Schedule**. For recurring reports, the report runs at the current time at the specified **Execution Frequency**.

5. Specify how often this report should run with the **Execution Frequency** drop-down list.
   Subsequent executions of this report occur at the time specified in the **First Execution** fields.

6. Click **Schedule** to save this scheduled report.
   Navigate to the Schedule Reports page to view a list of all scheduled reports in the **IdentityIQ** application.

   See "Scheduled Reports Tab" on page 179

How to Complete Report Work Items

Report work items are generated by reports that require sign off on the results they create and those sign off requests that are forwarded by a designated signer.

Sign off decisions are retained with the report results for tracking purposes.

Procedure

1. Click **My Work** in the Navigation menu to view your current work items.

2. Click a sign off type work item to display the sign off request.

3. Review the work item information in the Summary section.

4. Review the Comments section for any information associated with this work item.
    Use the **Add Comment** button to add additional information to the work item if necessary.

5. In the Details sections, click **Click to View Report Results** to display the Report Results page.

6. After you complete your review of the report results, click **Return to Work Item**.

7. Click an action button to open the associated comments dialog and conclude this work session.

    Note: **If you sign off or reject the sign-off request, the status of the report results is updated to reflect that decision. If you forward the work item, you must specify a recipient.**

Report List

SailPoint provides a number of standard reports that can be run without changes. You can also use the standard reports to create custom reports that are specific to your needs. Use scope to control access to your report results.

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off. The Report Layout configuration procedure is the same for all reports. See the following:

- "Standard Report Properties" on page 193.
- "Report Layout" on page 194.

The reports are divided in to the following categories:

- "Access Review and Certification Reports" on page 195
- "Account Group Reports" on page 197
- "Activity Reports" on page 211
- "Administration Reports" on page 213
- "Application Reports" on page 1
- "Configured Resource Reports" on page 224
- "Identity and User Reports" on page 228
- *****"Lifecycle Manager Reports" on page 305
- "Policy Enforcement Reports" on page 252
- "Risk Reports" on page 253
- "Role Management Reports" on page 258

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

*Requires Lifecycle Manager (sold separately)

Standard Report Properties

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and required sign off.

> **Note:** **The Name field is required for all reports, the other standard properties are optional.**

Enter or edit the standard properties information as required when creating or editing a report.

Table 4—Report - Standard Properties Descriptions

Field	Description
Name	Name of the report.
Description	Brief description of the report.
Require Signoff	Require sign off on the results of this task. Tasks that require sign off generate work items and email notifications that are assigned to the designated signers. Sign off decisions are retained with the task results for tracking purposes.
Previous Result Action	Previous result actions determine how subsequent runs of this task react to existing task results. **Delete** — overwrite the previous task results with the new information. **Rename Old** — append a numeral to the name of the old task result. **Rename New** — append a numeral to the name of the new task result. **Cancel** — cancel the new run of the task if a task result with the same name exists.
Allow Concurrency	Enable two identical tasks to run at the same time. If enabled, allow concurreny appends a numeric value to the name of the task that started second. If disabled, the second task is canceled and an exception sent to the requester.
Email Recipient	Specify a user or workgroup to whom an email should be sent when the report is finished running. Sending an email notification removes the need to log in to the product to check the progress of long running reports or reports that are scheduled to run periodically.
Email Attachment Format	Select either or both check boxes for PDF or CSV to have the report include an attachment copy. Clear the check boxes to not receive an attachment.
Maximum results to display	Set the maximum number of results to display in the results report. This option is available on a limited number of reports.
Scope	Set the scope for this report. Scope control access. Only identities that control the scope specified can see the results of this report. **Note: The scope information is not available for all reports. For those reports that support this feature, the Administrator must enable and configure the scope option.**

• For a list of available report templates, see "Report List" on page 192.

Report Layout

The Report Layout section of the Summary panel on the Edit Reports page is used to design the visible structure of your reports.

Table 5—Report Layout Descriptions

Field	Description
Sort by	Use the drop-down list to select the criteria by which the report is sorted.
Group by	Use the drop-down list to select the criteria by which the report is grouped. The resulting report displays the data in collapsible groups.
Columns	The column names to the right comprise of all possible columns the report can contain. Click to select a column name and either drag and drop or use the up / down arrow keys to arrange the order in which you would like the columns to appear in the report. To preclude a column from appearing, click to select the column name then click the left arrow button to move it to the panel on the left. Any column names in the right panel appear in the final report.
Disable Report Summary Display	Select this option to disable the display of a summary in the report results.
Disable Report Detail Display	Select this option to disable the display of a report details in the report results.

- For a list of available report templates, see "Report List" on page 192.

Access Review and Certification Reports

- "Access Review Decision Report" on page 195.
- "Access Review Signoff Live Report" on page 196.
- "Account Group Access Review Live Report" on page 198.
- "Advanced Access Review Live Report" on page 199.
- "Application Owner Access Review Live Report" on page 201.
- "Certification Activity by Application Report" on page 202.
- "Entitlement Owner Access Review Live Report" on page 204
- "Manager Access Review Live Report" on page 205.
- "Role Access Review Live Report" on page 207.

Access Review Decision Report

The Access Review Decision Report includes information about the decisions made by certifiers for all items in non-archived access reviews that match the report criteria.

This report is an archive-type report. Archive reports include end-of-period and task information that is formatted for easy dissemination of key audit information.Due to the large amount of data that is generated, the best option is to export the report results to a .pdf file.

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

See "Standard Report Properties" on page 193.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Report Criteria

The following criteria determines what information is included in this report.You can use any combination of options to build a report.

> **Note:** Selecting NO options from a list indicates that ALL options in the list are included in the report.

Table 6—Access Review Decision Report Options

Option	Description
Creation Start and End Date(s)	The access review creation date range. The report includes all access reviews create on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Signed Start and End Date(s)	The access review signed off on date range. The report includes all access reviews signed off on, on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Due Start and End Date(s)	The access review due date range. The report includes all access reviews due on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Tags	To filter access reviews based on their tags, select one or more tags. If multiple tags are selected, only access reviews that match all selected tags are included in this report.
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Managers	The manager list to include in this report. If no managers are specified, access reviews for all managers are included. Click the arrow to the right of the suggestion field to display a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.

Access Review Signoff Live Report

The Access Review Signoff Live Report includes information on who signed-off on a access review and if the signoff was completed.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Access Review Signoff Live Report consists of the following sections:

- Standard Properties
- Certification Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Certification Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> **Note:** Selecting NO options from a list indicates that ALL options in the list are included in the report.

Table 7—Access Review Signoff Live Report Certification Properties

Option	Description
Creation Start and End Date(s)	The access review creation date range. The report includes all access reviews create on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Signed Start and End Date(s)	The access review signed off on date range. The report includes all access reviews signed off on, on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Due Start and End Date(s)	The access review due date range. The report includes all access reviews due on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Managers	The manager list to include in this report. If no managers are specified, access reviews for all managers are included. Click the arrow to the right of the suggestion field to display a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.

Table 7—Access Review Signoff Live Report Certification Properties

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string. Only access reviews for account groups on the selected applications are included in the report.
Groups	The groups to include in the report. Click the "x" next to an item in the inclusion list to remove it from the report.
Certification Tags	To filter access reviews based on their tags, select one or more tags. If multiple tags are selected, only access reviews that match all selected tags are included in this report.
Certification Group	The manager certifications to include in this report.
Signed Off	Filter by the signed off status of certifications.
E-Signed	Use this field to filter results by certifications that include an electronic signature.

Account Group Access Review Live Report

The Account Group Access Review Live Report includes information about all account group access reviews in IdentityIQ.

> **Note:** **You must generate separate reports for account group membership and permissions access reviews.**

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Account Group Access Review Live Report consists of the following sections:

- Standard Properties
- Certification Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name
- Applications from the list
- Account group access review type - Membership or Permissions

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Certification Properties

The following criteria determines what information is included in this report.You can use any combination of options to build a report.

Note: Selecting NO options from a list indicates that ALL options in the list are included in the report.

Table 8—Account Group Access Review Live Report Certification Properties

Option	Description
Creation Start and End Date(s)	The access review creation date range. The report includes all access reviews create on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Signed Start and End Date(s)	The access review signed off on date range. The report includes all access reviews signed off on, on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Due Start and End Date(s)	The access review due date range. The report includes all access reviews due on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Applications	The applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string. Only access reviews for account groups on the selected applications are included in the report.
Certification Tags	To filter access reviews based on their tags, select one or more tags. If multiple tags are selected, only access reviews that match all selected tags are included in this report.
Certification Groups	The type of Account Group access reviews to include in this report, Membership or Permissions.
Show excluded items	Select this check box to include any excluded items in the report. **Note: This option disable the preview grid view.**

Advanced Access Review Live Report

The Advanced Access Review Live Report includes information on all non-archived advanced access reviews that match the criteria specified.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Advanced Access Review Live Report consists of the following sections:
- Standard Properties
- Certification Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:
- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Certification Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Note: **Selecting NO options from a list indicates that ALL options in the list are included in the report.**

Table 9—Advanced Access Review Live Report Certification Properties

Option	Description
Creation Start and End Date(s)	The access review creation date range. The report includes all access reviews create on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Signed Start and End Date(s)	The access review signed off on date range. The report includes all access reviews signed off on, on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Due Start and End Date(s)	The access review due date range. The report includes all access reviews due on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.

Table 9—Advanced Access Review Live Report Certification Properties

Option	Description
Groups	The groups or populations to include in the report. Click the arrow to the right of the field and select **Populations**, to display a select list of populations, or select a group factory name to display a select list of groups created by that factory. Click on populations and groups from the select lists to create the inclusion list for this report. Click an item in the inclusion list to remove it from the report.
Certification Tags	To filter access reviews based on their tags, select one or more tags. If multiple tags are selected, only access reviews that match all selected tags are included in this report.
Certification Group	The manager certifications to include in this report.
Show excluded items	Select this check box to include any excluded items in the report. **Note: This option disable the preview grid view.**

Application Owner Access Review Live Report

The Application Owner Access Review Live Report includes information on all non-archived application owner access reviews that match the criteria specified.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Application Owner Access Review Report consists of the following sections:

• Standard Properties
• Certification Properties
• Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

• Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Certification Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Note: Selecting NO options from a list indicates that ALL options in the list are included in the report.

Table 10—Application Owner Access Review Live Report Certification Properties

Option	Description
Creation Start and End Date(s)	The access review creation date range. The report includes all access reviews create on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Signed Start and End Date(s)	The access review signed off on date range. The report includes all access reviews signed off on, on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Due Start and End Date(s)	The access review due date range. The report includes all access reviews due on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string. Only access reviews for the selected applications are included in the report.
Certification Tags	To filter access reviews based on their tags, select one or more tags. If multiple tags are selected, only access reviews that match all selected tags are included in this report.
Certification Group	The manager certifications to include in this report.
Show excluded items	Select this check box to include any excluded items in the report. **Note: This option disable the preview grid view.**

Certification Activity by Application Report

The Certification Activity by Application Report includes information activity performed on non-archived certifications that match the specified criteria.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Certification Activity by Application Report consists of the following sections:

- Standard Properties
- Certification Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name
- Application from the list

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Certification Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Note: **Selecting NO options from a list indicates that ALL options in the list are included in the report.**

Table 11—Certification Activity by Application Report Certification Properties

Option	Description
Creation Start and End Date(s)	The access review creation date range. The report includes all access reviews create on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Signed Start and End Date(s)	The access review signed off on date range. The report includes all access reviews signed off on, on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Due Start and End Date(s)	The access review due date range. The report includes all access reviews due on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string. Only access reviews for the selected applications are included in the report.

Option	Description
Certification Tags	To filter access reviews based on their tags, select one or more tags. If multiple tags are selected, only access reviews that match all selected tags are included in this report.
Certification Group	The manager certifications to include in this report.
Show excluded items	Select this check box to include any excluded items in the report. **Note: This option disable the preview grid view.**

Entitlement Owner Access Review Live Report

The Entitlement Owner Access Review Live Report includes information on all non-archived entitlement owner access reviews that match the criteria specified.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Entitlement Owner Access Review Report consists of the following sections:

- Standard Properties
- Certification Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Certification Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Note: **Selecting NO options from a list indicates that ALL options in the list are included in the report.**

Table 12—Entitlement Owner Access Review Live Report Certification Properties

Option	Description
Creation Start and End Date(s)	The access review creation date range. The report includes all access reviews create on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Signed Start and End Date(s)	The access review signed off on date range. The report includes all access reviews signed off on, on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Due Start and End Date(s)	The access review due date range. The report includes all access reviews due on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string. Only access reviews for the selected applications are included in the report.
Certification Tags	To filter access reviews based on their tags, select one or more tags. If multiple tags are selected, only access reviews that match all selected tags are included in this report.
Certification Group	The manager certifications to include in this report.
Show excluded items	Select this check box to include any excluded items in the report. **Note: This option disable the preview grid view.**

Manager Access Review Live Report

The Manager Access Review Report includes information on all non-archived manager access reviews that match the criteria specified.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

The Manager Access Review Report consists of the following sections:

- Standard Properties
- Certification Properties
- Report Layout

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Certification Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Note: **Selecting NO options from a list indicates that ALL options in the list are included in the report.**

Table 13—Manager Access Review Report Certification Properties

Option	Description
Creation Start and End Date(s)	The access review creation date range. The report includes all access reviews create on or after the start date and on or before the end date. You can enter the date manually, or click the **"…"** icon to select a date from the calendar.
Signed Start and End Date(s)	The access review signed off on date range. The report includes all access reviews signed off on, on or after the start date and on or before the end date. You can enter the date manually, or click the **"…"** icon to select a date from the calendar.
Due Start and End Date(s)	The access review due date range. The report includes all access reviews due on or after the start date and on or before the end date. You can enter the date manually, or click the **"…"** icon to select a date from the calendar.
Managers	The manager list to include in this report. If no managers are specified, access reviews for all managers are included. Click the arrow to the right of the suggestion field to display a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.
Certification Tags	To filter access reviews based on their tags, select one or more tags. If multiple tags are selected, only access reviews that match all selected tags are included in this report.

Table 13—Manager Access Review Report Certification Properties

Option	Description
Certification Group	The manager certifications to include in this report.
Show excluded items	Select this check box to include any excluded items in the report. **Note: This option disable the preview grid view.**

Role Access Review Live Report

The Role Access Review Report includes information about all role access reviews in IdentityIQ.

> **Note:** You must generate separate reports for Role Membership and Role Composition access reviews.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Role Access Review Report consists of the following sections:

- Standard Properties
- Certification Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name
- Role
- Role access review type - Membership or Composition

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Certification Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> **Note:** Selecting NO options from a list indicates that ALL options in the list are included in the report.

Table 14—Role Access Review Certification Properties

Option	Description
Creation Start and End Date(s)	The access review creation date range. The report includes all access reviews create on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Signed Start and End Date(s)	The access review signed off on date range. The report includes all access reviews signed off on, on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Due Start and End Date(s)	The access review due date range. The report includes all access reviews due on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Roles	The roles to include in the report. If no roles are specified, all roles are included. Click the arrow to the right of the suggestion field to display a list of all roles, or enter a few letters in the field to display a list of roles that start with that letter string.
Certification Tags	To filter access reviews based on their tags, select one or more tags. If multiple tags are selected, only access reviews that match all selected tags are included in this report.
Certification Group	The type of role certifications to include in this report; Membership or Composition.
Show excluded items	Select this check box to include any excluded items in the report. **Note: This option disable the preview grid view.**

Targeted Access Review Live Report

The Targeted Access Review Live Report includes information about all targeted access reviews in IdentityIQ.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Targeted Access Review Live Report consists of the following sections:

- Standard Properties
- Certification Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Certification Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> **Note:** Selecting NO options from a list indicates that ALL options in the list are included in the report.

Table 15—Role Access Review Certification Properties

Option	Description
Creation Start and End Date(s)	The access review creation date range. The report includes all access reviews create on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Signed Start and End Date(s)	The access review signed off on date range. The report includes all access reviews signed off on, on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Due Start and End Date(s)	The access review due date range. The report includes all access reviews due on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Certification Tags	To filter access reviews based on their tags, select one or more tags. If multiple tags are selected, only access reviews that match all selected tags are included in this report.
Certification Group	The type of role certifications to include in this report; Membership or Composition.

Account Group Reports

Account Group Members Report

The Account Group Members Report includes information about all the members of all the account groups and application objects.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Account Group Members Report consists of the following sections:

- Standard Properties
- Report Options
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name
- Application
- Member Options

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Report Options

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> **Note:** **Selecting NO options from a list indicates that ALL options in the list are included in the report.**

Table 16—Account Group Membership Report Options

Option	Description
Application	Select which application to include in the report.

Account Group Membership Totals Report

The Account Group Membership report includes information about all account groups and application object types in your system and their members.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Account Group Membership Report consists of the following sections:

- Standard Properties
- Report Options
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name
- Application
- Member Options

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Report Option

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> **Note:** **Selecting NO options from a list indicates that ALL options in the list are included in the report.**

Table 17—Account Group Membership Report Options

Option	Description
Application	Select which application to include in the report.

Activity Reports

User Activity Report

The User Activity Detailed Report includes information on all activity on the applications monitored by IdentityIQ according to the criteria specified.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The User Activity Report consists of the following sections:

- Standard Properties
- Additional Identity Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Additional Identity Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> **Note:** Selecting NO options from a list indicates that ALL options in the list are included in the report.

Table 18—User Activity Additional Identity Properties Options

Option	Description
Identities	The identity list to include in this report. If no identities are specified, activity for all identities is included. Click the arrow to the right of the suggestion field to display a list of all identities, or enter a few letters in the field to display a list of identities that start with that letter string.
Applications	Select the applications to include in the report. If no applications are specified, all applications configured to track activity are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Start and End Dates	The first and last date for which activity is reported. The report includes all application activity that occurred within the date range specified. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Action	The actions to include in the report. Only activity of the action types selected are included in the report. Use the Ctrl and Shift keys to select multiple actions.
Result	The activity results to include in the report. Only activities that include the selected result, Success or Failure, are included.
Target	The specific target on an application to include in the report. Use the target filter to further narrow the result set for a search on a specific application.

Administration Reports

- "Capabilities to Identities Report" on page 213
- "Connectivity Information Report" on page 214
- "Detailed Provisioning Transaction Object Report" on page 215
- "Environment Information Report" on page 216.
- "Identity to Capabilities Report" on page 217
- "Mitigation Report" on page 218.
- "Provisioning Transaction Object Report" on page 219
- "Revocation Live Report" on page 220.
- "Work Item Archive Report" on page 222.

Capabilities to Identities Report

The Capabilities to Identities Report displays a list of the identities assigned to each capability defined in your enterprise.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Capabilities to Identities Report consists of the following sections:
- Standard Properties
- Capability Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:
- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Capabilities Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> **Note:** Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Capabilities	The capabilities to include in the report.
Exclude Indirect Capabilities	Do not include identities that have the capability assigned indirectly, through a workgroup.
Exclude Workgroups	Do not include workgroups in the report results.

Connectivity Information Report

The Connectivity Information Report displays all of the information collected about application configurations and statistics that match the specified criteria.

This report collects the following information:

- Application configuration attributes and schema from Application xml.
- Last aggregation run time for all type of aggregations such as, Account aggregation, Group aggregation, and Delta aggregation.
- Average time taken for all type of aggregations.
- Schedule frequency for all type of aggregations.
- Provisioning operations statistics such as, number of create, update, and change password.
- Total accounts and groups.
- Maximum and average entitlements per account.
- Maximum and average members per group.

> **Note:** **Remove sensitive data before exporting.**

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Connectivity Information Report consists of the following sections:

- Standard Properties
- Application Filter
- Attributes Filter
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Application Filter

Specify applications to exclude from this report. You can exclude applications by type or name. For excluded application, only statistical information is collected. Application configuration details are ignored for excluded applications.

Attribute Filter

Specify attributes to exclude from this report. The values of the application attributes displayed in the list are not included in the report.

Detailed Provisioning Transaction Object Report

The Detailed Provisioning Transaction Object Report displays all of the information for all of the provisioning transactions in the system that match the specified criteria.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Detailed Provisioning Transaction Object Report consists of the following sections:

- Standard Properties
- Provisioning Transaction Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Provisioning Transaction Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> **Note:** **Selecting NO options from a list indicates that ALL options in the list are included in the report.**

Table 20—Detailed Provisioning Transaction Object Report Properties

Option	Description
Application	The applications list to include in this report. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Identities	The identities list to include in this report. Click the arrow to the right of the suggestion field to display a list of all identities, or enter a few letters in the field to display a list of identities that start with that letter string.
Channel	The channels list to include in this report. Click the arrow to the right of the suggestion field to display a list of all available channels, or enter a few letters in the field to display a list of channels that start with that letter string.
Account	Limit returned provisioning transactions to those with the account display name begins with value entered in this field.
Event	The events list to include in this report. Click the arrow to the right of the suggestion field to display a list of all available events, or enter a few letters in the field to display a list of events that start with that letter string.
Source	The source list to include in this report. Click the arrow to the right of the suggestion field to display a list of all available sources, or enter a few letters in the field to display a list of sources that start with that letter string.
Status	The status list to include in this report. Click the arrow to the right of the suggestion field to display a list of all available statuses, or enter a few letters in the field to display a list of statuses that start with that letter string.
Type	Select Manual or Auto to limit the results of this report by transaction type.
Transaction Initiation Date	Limit the report results by date range.
Overridden	Only include provisioning transactions that were manually overwritten on the Provisioning Transaction Table.

Environment Information Report

The Environment Information Report displays information about user activity on each application in detailed format (statistics about IdentityIQ environment).

The Environment Information Report consists of the following sections:

- Standard Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

-

Identity to Capabilities Report

The Identity to Capabilities Report displays a list of the capabilities assigned to each identity in your enterprise.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Capabilities to Identities Report consists of the following sections:

- Standard Properties
- Capability Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Identity Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> **Note:** **Selecting NO options from a list indicates that ALL options in the list are included in the report.**

Table 21—Identities to Capabilities **Report Properties**

Option	Description
Identities	The identities to include in the report.

Table 21—Identities to Capabilities **Report Properties**

Option	Description
Include Empty Capabilities	Include identities that have no assigned capabilities.
Exclude Indirect Capabilities	Do not include capabilities assigned through workgroups in the report results.
Exclude Workgroups	Do not include workgroups in the report results.

Mitigation Report

The Mitigation Report includes information on all mitigations in the system that match the specified criteria.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Mitigation Report consists of the following sections:

- Standard Properties
- Mitigation Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Mitigation Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Note: Selecting NO options from a list indicates that ALL options in the list are included in the report.

Table 22—Mitigation Report Properties

Option	Description
Expiration Date	The expiration limit on the exception. Exceptions that expire on dates up to and including the selected date are included in this report. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Identities	The identities list to include in this report. If no identities are specified, mitigation for all identities are included. Click the arrow to the right of the suggestion field to display a list of all identities, or enter a few letters in the field to display a list of identities that start with that letter string.
Actors	The manager (mitigator) list to include in this report. If no managers are specified, mitigations for all managers are included. Click the arrow to the right of the suggestion field to display a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.
Business Roles	The roles list to include in this report. If no roles are specified, mitigation on all roles are included. Click the arrow to the right of the suggestion field to display a list of all roles, or enter a few letters in the field to display a list of roles that start with that letter string.

Provisioning Transaction Object Report

The Provisioning Transaction Object Report displays all of the provisioning transactions in the system that match the specified criteria.

The Provisioning Transaction Object Report consists of the following sections:

- Standard Properties
- Provisioning Transaction Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Provisioning Transaction Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> **Note:** **Selecting NO options from a list indicates that ALL options in the list are included in the report.**

Table 23—Provisioning Transaction Object Report Properties

Option	Description
Application	The applications list to include in this report. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Identities	The identities list to include in this report. Click the arrow to the right of the suggestion field to display a list of all identities, or enter a few letters in the field to display a list of identities that start with that letter string.
Channel	The channels list to include in this report. Click the arrow to the right of the suggestion field to display a list of all available channels, or enter a few letters in the field to display a list of channels that start with that letter string.
Account	Limit returned provisioning transactions to those with the account display name begins with value entered in this field.
Event	The events list to include in this report. Click the arrow to the right of the suggestion field to display a list of all available events, or enter a few letters in the field to display a list of events that start with that letter string.
Source	The source list to include in this report. Click the arrow to the right of the suggestion field to display a list of all available sources, or enter a few letters in the field to display a list of sources that start with that letter string.
Status	The status list to include in this report. Click the arrow to the right of the suggestion field to display a list of all available statuses, or enter a few letters in the field to display a list of statuses that start with that letter string.
Type	Select Manual or Auto to limit the results of this report by transaction type.
Transaction Initiation Date	Limit the report results by date range.
Overridden	Only include provisioning transactions that were manually overwritten on the Provisioning Transaction Table.

Revocation Live Report

The Revocation Live Report includes information on all revocations in the system that match the specified criteria.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Revocation Live Report consists of the following sections:

- Standard Properties
- Certification Item Properties
- Report Layout

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Certification Items Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> **Note:** Selecting NO options from a list indicates that ALL options in the list are included in the report.

Table 24—Revocation Report Certification Items Properties Options

Option	Description
Creation Start and End Date(s)	The certification creation date range. The report includes all revocation information for certifications create on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Signed Start and End Date(s)	The certification signed off on date range. The report includes all revocation information for certifications signed off on, on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Due Start and End Date(s)	The certification due date range. The report includes all revocation information for certifications due on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Group	Select the groups to include in this report. Click the arrow to the right of the suggestion field to display a list of all groups, or enter a few letters in the field to display a list of groups that start with that letter string.

Table 24—Revocation Report Certification Items Properties Options

Option	Description
Certification Tags	To filter access reviews based on their tags, select one or more tags. If multiple tags are selected, only access reviews that match all selected tags are included in this report.
Certification Group	The manager certifications to include in this report.

Work Item Archive Report

The Work Item Archive Report includes information on all work items in the system that match the specified criteria.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Work Item Archive Report consists of the following sections:

- Standard Properties
- Work Item Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Work Item Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Note: Selecting NO options from a list indicates that ALL options in the list are included in the report.

Table 25—Work Item Archive Report Work Item Properties

Option	Description
Owners	The owners of the work items. Only work items belonging to the selected owners are included in the report. Click the arrow to the right of the suggestion field to display a list of all owners, or enter a few letters in the field to display a list of owners that start with that letter string.
Requestors	The requestors of the work items. Only work items requested by the selected requestors are included in the report. Click the arrow to the right of the suggestion field to display a list of all requestors, or enter a few letters in the field to display a list of requestors that start with that letter string.
Work Items Priority	The priority assigned by the requestor of the work item.
Work Items Type	The work item types to include in this report. Only work items of the type selected are included in the report. Use the Shift and Ctrl buttons to select multiple types.
Work Item State	The state of the work items to include in this report. Only work items in the selected states are included in the report. Use the Shift and Ctrl buttons to select multiple states.
Included Work Items	Choose to include active or archived work items in the report.
Minimum Reminders	The minimum number of sent reminders that a work item must be associate with before it is included in this report.
Maximum Reminders	The maximum number of sent reminders that a work item can be associated with and still be included in this report.

Application Reports

Application Status Report

The Application Status Report includes information in detail format for applications that IdentityIQ monitors.

This report includes information in the detailed results format that can be exported to Microsoft Excel and used as spreadsheets.

The Application Status Report consists of the following sections:

• Standard Properties

• Report Options

• Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must assign a name before running this report:

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Report Options

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

- Applications

Select the applications to include in the report. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.

>   **Note:** **Selecting NO options from a list indicates that ALL options in the list are included in the report.**

Report Data

The Application Status Report displays the following data:

- Application
- Number of Accounts
- Last Aggregation
- Oldest Refresh Time
- Newest Refresh Time
- Total Assignments
- Unique Entitlements

Configured Resource Reports

- See "Configured Applications Archive Report" on page 224
- See "Configured Applications Detail Report" on page 225
- See "Delimited File Application Status Report" on page 226

Configured Applications Archive Report

The Configured Applications Archive report includes information about all of the applications that match the specified criteria.

This report is an archive-type report. Archive reports include end-of-period and task information that is formatted for easy dissemination of key audit information.Due to the large amount of data that is generated, the best option is to export the report results to a .pdf file.

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Application Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> **Note:**   **Selecting NO options from a list indicates that ALL options in the list are included in the report.**

Table 26—Configured Applications Archive Report Options

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Owners	The application owners to include in the report. Only applications associated with selected application owners are included in the report Click the arrow to the right of the suggestion field to display a list of all owners, or enter a few letters in the field to display a list of owners that start with that letter string.

Configured Applications Detail Report

The Configured Applications Detail report includes information about all of the applications that match the specified criteria.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Configured Applications Detail Report consists of the following sections:

- Standard Properties
- Application Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Application Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> **Note:** **Selecting NO options from a list indicates that ALL options in the list are included in the report.**

Table 27—Configured Applications Detail Report Application Properties Options

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Owners	The application owners to include in the report. Only applications associated with selected application owners are included in the report Click the arrow to the right of the suggestion field to display a list of all owners, or enter a few letters in the field to display a list of owners that start with that letter string.

Delimited File Application Status Report

The Delimited File Application Status Report includes information about applications that are of type Delimited File Parsing Connector and that also have local file types. For example, applications that use delimited files, but are acquired through a proxy such as ftp are not shown in the report.

This report includes a Refresh Date indicating the date on which the last application aggregation was begun. The report does not include information on the end date of that aggregation or if it was successful. Therefore this report should not be used as an indicator of application aggregation success.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Delimited File Application Status Report consists of the following sections:

- Standard Properties
- Delimited File Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Delimited File Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> **Note:** **Selecting NO options from a list indicates that ALL options in the list are included in the report.**

Table 28—Delimited File Application Status Report Options

Option	Description
Application	Select which application to include in the report.

Identity and User Reports

Account Attributes Live Report

The Account Attributes Live Report includes a detailed view of each identity and the entitlements that they are assigned. The report searches the identity cubes to extract the desired information.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Account Attributes Live Report consists of the following sections:
- Standard Properties
- Identity Attributes
- Identity Properties
- Report Layout

> **Note:** **Based on how IdentityIQ was set up for your enterprise, other attributes may be available. Extended attributes may include items such as region, location, department, and other attributes specific to your deployment.**

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:
- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Identity Attributes

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> **Note:** Selecting NO options from a list indicates that ALL options in the list are included in the report.

> **Note:** Use the Shift and Crtl keys to select multiple items from lists.

Table 29—Account Attributes Live Report Identity Attributes

Option	Description
User Attributes	The user attributes on which to filter. Only users with the listed attributes are included in the report. This information is discovered during identity aggregation. **Note: Identity attributes can be configured. The attributes that display can vary for each instance of the product.**
First Name	Input the first name of the identity you wish the report to include. For example, if you input "John" in the field, the report includes information on identities whose first name is John.
Last Name	Input the last name of the identity you wish the report to include. For example, if you input "Smith" in the field, the report includes information on identities whose last name is Smith.
Display Name	Input the display name of the identity you wish the report to include. For example, if you input "John_Smith" in the field, the report includes information on identities whose display name is John_Smith.
Email	Input the email address of the identity you wish the report to include. For example, if you input "John@email.com" in the field, the report includes information on identities whose email address is name is John@email.com.
Manager	The manager list to include in this report. Only users who report to the selected managers are included in the report. Click the arrow to the right of the suggestion field to a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.
Inactive	Choose how the report handles inactive users. Select **No selection** to include both inactive and active users, **True** to include only inactive users, or **False** to not include inactive users.

Identity Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> **Note:** Selecting NO options from a list indicates that ALL options in the list are included in the report.

> **Note:** Use the Shift and Crtl keys to select multiple items from lists.

Table 30—Account Attributes Live Report Identity Properties

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Capabilities	Select the capabilities to include in the report.
Groups	The groups or populations to include in the report. Click the arrow to the right of the field and select a group to create the inclusion list for this report.
Last Refresh Date	Select a date range to filter users based on when the user was last refreshed.
Last Login Date	Specify a login date range manually or click the calendar icon and select one using the calendar options.
Show authorized scopes and capabilities	Select this option to include authorized scopes and capabilities for each identity in the report.

Application Account Summary Report

The Application Account Summary Report includes a summary of all accounts on each application.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Application Account Summary Report consists of the following sections:
- Standard Properties
- Report Options
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:
- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Report Options

The following criteria determines what information is included in this report.

Table 31—Application Account Summary Report Options

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.

Note: Selecting NO options from a list indicates that ALL options in the list are included in the report.

Note: Use the Shift and Crtl keys to select multiple items from lists.

Application Account by Attribute Report

The Application Account by Attribute Report includes information on accounts that are on extended account attributes.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Application Account by Attribute Report consists of the following sections:

- Standard Properties
- Account Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Account Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Note: Selecting NO options from a list indicates that ALL options in the list are included in the report.

Table 32—Application Account by Attribute Account Properties

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Inactive Account	Choose how the report handles inactive accounts. Select **No selection** to include both inactive and active accounts, **True** to include only inactive accounts, or **False** to not include inactive accounts.
Privileged Account	Choose how the report handles privileged accounts. Select **No selection** to include both privileged and standard accounts, **True** to include only privileged accounts, or **False** to not include privileged accounts.
Service Account	Choose how the report handles service accounts. Select **No selection** to include both service and standard accounts, **True** to include only service accounts, or **False** to not include service accounts.
Last login	Specify a login date range manually or click the calendar icon and select one using the calendar options.

Identity Effective Access Live Report

The Identity Effective Access Live Report includes a high-level view of all entitlements a user has and how the user received those entitlements.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Identity Effective Access Live Report consists of the following sections:
- Standard Properties
- Identity Attributes
- Identity Extended Attributes
- Additional Identity Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:
- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Identity Attributes

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Table 33— Identity Effective Access Live Report Identity Attributes Options

Option	Description
First Name	Input the first name of the identity you wish the report to include. For example, if you input "John" in the field, the report includes information on identities whose first name is John.
Last Name	Input the last name of the identity you wish the report to include. For example, if you input "Smith" in the field, the report includes information on identities whose last name is Smith.
Display Name	Input the display name of the identity you wish the report to include. For example, if you input "John_Smith" in the field, the report includes information on identities whose display name is John_Smith.
Email	Input the email address of the identity you wish the report to include. For example, if you input "John@email.com" in the field, the report includes information on identities whose email address is name is John@email.com.
Manager	The manager list to include in this report. Only users who report to the selected managers are included in the report. Click the arrow to the right of the suggestion field to a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.
Inactive	Choose how the report handles inactive identities. Select **No selection** to include both inactive and active identities, **True** to include only inactive identities, or **False** to not include inactive identities.

Identity Extended Attributes

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Table 34—Identity Effective Access Live Report Identity Extended Attributes Options

Option	Description
Region	The user attributes on which to filter. Only users with the listed attributes are included in the report. This information is discovered during identity aggregation. **Note: Identity attributes are configurable and the attributes displayed might vary for each instance of the product.**

Table 34—Identity Effective Access Live Report Identity Extended Attributes Options

Option	Description
Department	The manager list to include in this report. Only users who report to the selected managers are included in the report. Click the arrow to the right of the suggestion field to display a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.
Location	The groups or populations to include in the report. Click the arrow to the right of the field and select **Populations**, to display a select list of populations, or select a group factory name to display a select list of groups created by that factory. Click on populations and groups from the select lists to create the inclusion list for this report. Click an item in the inclusion list to remove it from the report.
Employee ID	Select an operator from the list, Before or After, and specify a date manually or click the **"..."** icon and select one using the calendar options. Optionally include identities that have never been refresh.
Job Title	Select an operator from the list, Before or After, and specify a date manually or click the **"..."** icon and select one using the calendar options. Optionally include identities that have never logged in to the product.
Region Owner	Specify that the report should include only active or only inactive identities.
Location Owner	The roles to include in the report. If no roles are specified, all roles are included. Click the arrow to the right of the suggestion field to display a list of all roles, or enter a few letters in the field to display a list of roles that start with that letter string.
DN	Specify a unique name for the Distinguished Name.
Cost Center	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Match Mode	Select the capabilities to include in the report.

Additional Identity Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Table 35—Identity Effective Access Live Report Additional Identity Properties Options

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Capabilities	Select the capabilities to include in the report.

Table 35—Identity Effective Access Live Report Additional Identity Properties Options

Option	Description
Roles	The roles to include in the report. Click the arrow to the right of the field and select a role to create the inclusion list for this report.
Groups	The groups or populations to include in the report. Click the arrow to the right of the field and select a group to create the inclusion list for this report.
Last Refresh Date	Select a date range to filter users based on when the user was last refreshed.
Last Login Date	Select a date range to filter users based on when the user was last logged in.

Identity Entitlements Detail Report

Note: **Including classifications in the Identity Entitlements Detail Report can impact performance. By default, classifications are included in this report, but you can remove them in the Report Layout dialog.**

The Identity Entitlements Detail Report includes information on user and their associated attributes. The report searches the identity cubes to extract the desired information.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Identity Entitlements Detail Report consists of the following sections:

• Standard Properties

• Identity Entitlements Detail Report Arguments

• Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

• Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Identity Entitlements Report Arguments

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Note: **Selecting NO options from a list indicates that ALL options in the list are included in the report.**

Note: Use the Shift and Crtl keys to select multiple items from lists.

Option	Description
Identities	Type in manually or use the drop-down list to select the identities to include in the report. If no identities are specified, all identities are included.
Applications	Type in manually or use the drop-down list to select the applications to include in the report. If no applications are specified, all applications are included.
Attributes	Type in manually or use the drop-down list to select the attributes to include in the report. If no attributes are specified, all attributes are included.
Entitlements	Type in manually or use the drop-down list to select the entitlements to include in the report. If no entitlements are specified, all entitlements are included.
Accounts	Type in manually or use the drop-down list to select the accounts to include in the report. If no accounts are specified, all accounts are included.
Instances	Type in manually or use the drop-down list to select the instances to include in the report. If no instances are specified, all instances are included.
Assigners	Type in manually or use the drop-down list to select the assigners to include in the report. If no assigners are specified, all assigners are included.
Source	Type in manually or use the drop-down list to select the sources to include in the report. If no sources are specified, all sources are included.
Exists on account	Select **Include All** to include all entitlements **True** to include only entitlements that were found on the last aggregation, or **False** to not include entitlements that were found on the last aggregation.
Entitlement Type	Select from **Include All**, **Entitlements**, or **Permissions**.
Allowed by an assigned role	Select **Include All** to include all entitlements **True** to include only entitlements that were not granted by a role, or **False** to preclude entitlements that were not granted by a role.
Additional Entitlements only	Select **Include All** to include all entitlements **True** to include only entitlements that were allowed by an assigned role, or **False** to not include entitlements that allowed by an assigned role.
Has been certified	Select **Include All** to include all entitlements **True** to include only entitlements that have been certified, or **False** to not include entitlements that have been certified.
Has pending certification	Select **Include All** to include all entitlements **True** to include only entitlements that have a pending certification, or **False** to not include entitlements that have a pending certification.
Has been requested	Select **Include All** to include all entitlements **True** to include only entitlements that have been requested, or **False** to not include entitlements that have been requested.
Has pending request	Select **Include All** to include all entitlements **True** to include only entitlements that have a pending request, or **False** to not include entitlements that have a pending request.

Identity Forwarding Report

The Identity Forwarding Report includes forwarding information for users who are configured for forwarding. The report searches the identity cubes to extract the desired information, including the start and end dates of the forwarding period.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Identity Forwarding Report consists of the following sections:

- Standard Properties
- Identity Attributes
- Identity Extended Attributes
- Additional Identity Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Identity Attributes

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Table 37— Identity Forwarding Report Identity Attributes Options

Option	Description
First Name	Input the first name of the identity you wish the report to include. For example, if you input "John" in the field, the report includes information on identities whose first name is John.
Last Name	Input the last name of the identity you wish the report to include. For example, if you input "Smith" in the field, the report includes information on identities whose last name is Smith.
Display Name	Input the display name of the identity you wish the report to include. For example, if you input "John_Smith" in the field, the report includes information on identities whose display name is John_Smith.

Option	Description
Email	Input the email address of the identity you wish the report to include. For example, if you input "John@email.com" in the field, the report includes information on identities whose email address is name is John@email.com.
Manager	The manager list to include in this report. Only users who report to the selected managers are included in the report. Click the arrow to the right of the suggestion field to a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.
Inactive	Choose how the report handles inactive identities. Select **No selection** to include both inactive and active identities, **True** to include only inactive identities, or **False** to not include inactive identities.

Identity Extended Attributes

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Table 38—Identity Forwarding Report Identity Extended Attributes Options

Option	Description
Region	The user attributes on which to filter. Only users with the listed attributes are included in the report. This information is discovered during identity aggregation. **Note: Identity attributes are configurable and the attributes displayed might vary for each instance of the product.**
Department	The manager list to include in this report. Only users who report to the selected managers are included in the report. Click the arrow to the right of the suggestion field to display a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.
Location	The groups or populations to include in the report. Click the arrow to the right of the field and select **Populations**, to display a select list of populations, or select a group factory name to display a select list of groups created by that factory. Click on populations and groups from the select lists to create the inclusion list for this report. Click an item in the inclusion list to remove it from the report.
Employee ID	Select an operator from the list, Before or After, and specify a date manually or click the **"..."** icon and select one using the calendar options. Optionally include identities that have never been refresh.
Job Title	Select an operator from the list, Before or After, and specify a date manually or click the **"..."** icon and select one using the calendar options. Optionally include identities that have never logged in to the product.
Region Owner	Specify that the report should include only active or only inactive identities.

Table 38—Identity Forwarding Report Identity Extended Attributes Options

Option	Description
Location Owner	The roles to include in the report. If no roles are specified, all roles are included. Click the arrow to the right of the suggestion field to display a list of all roles, or enter a few letters in the field to display a list of roles that start with that letter string.
DN	Specify a unique name for the Distinguished Name.
Cost Center	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Match Mode	Select the capabilities to include in the report.

Additional Identity Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Table 39—Identity Forwarding Report Additional Identity Properties Options

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Capabilities	Select the capabilities to include in the report.
Roles	The roles to include in the report. Click the arrow to the right of the field and select a role to create the inclusion list for this report.
Groups	The groups or populations to include in the report. Click the arrow to the right of the field and select a group to create the inclusion list for this report.
Last Refresh Date	Select a date range to filter users based on when the user was last refreshed.
Last Login Date	Select a date range to filter users based on when the user was last logged in.

Identity Status Summary Report

The Identity Status Summary Report includes summarized information on active, inactive and total identities detected by IdentityIQ.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

• Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Privileged User Access Report

The Privileged User Access Report includes detailed information on the privileged users detected by IdentityIQ.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Privileged User Access Report consists of the following sections:

• Standard Properties
• Privileged Account Attributes
• Account Applications
• Identity Attributes
• Identity Extended Attributes
• Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

• Name
• At least one Privileged Account Attribute

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Privileged Attributes

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Note: **Selecting NO options from a list indicates that ALL options in the list are included in the report.**

Note: Use the Shift and Crtl keys to select multiple items from lists.

Table 40—Privileged User Access Report Privileged Account Attributes Options

Option	Description
Inactive Account	Choose how the report handles inactive accounts. Select **No selection** to include both inactive and active accounts, **True** to include only inactive accounts, or **False** to not include inactive accounts.
Privileged Account	Choose how the report handles privileged accounts. Select **No selection** to include both privileged and standard accounts, **True** to include only privileged accounts, or **False** to not include privileged accounts.
Service Account	Choose how the report handles service accounts. Select **No selection** to include both service and standard accounts, **True** to include only service accounts, or **False** to not include service accounts.
Last Login Date	Select a date range to filter users based on when the user was last logged in.

Account Applications

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Note: Selecting NO options from a list indicates that ALL options in the list are included in the report.

Note: Use the Shift and Crtl keys to select multiple items from lists.

Table 41—Privileged User Access Report Account Applications

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.

Identity Attributes

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Note: Selecting NO options from a list indicates that ALL options in the list are included in the report.

Note: Use the Shift and Crtl keys to select multiple items from lists.

Table 42—Privileged User Access Report Identity Attributes

Option	Description
First Name	Input the first name of the identity you wish the report to include. For example, if you input "John" in the field, the report includes information on identities whose first name is John.

Table 42—Privileged User Access Report Identity Attributes

Option	Description
Last Name	Input the last name of the identity you wish the report to include. For example, if you input "Smith" in the field, the report includes information on identities whose last name is Smith.
Display Name	Input the display name of the identity you wish the report to include. For example, if you input "John_Smith" in the field, the report includes information on identities whose display name is John_Smith.
Email	Input the email address of the identity you wish the report to include. For example, if you input "John@email.com" in the field, the report includes information on identities whose email address is name is John@email.com.
Manager	The manager list to include in this report. Only users who report to the selected managers are included in the report. Click the arrow to the right of the suggestion field to a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.
Inactive	Choose how the report handles inactive users. Select **No selection** to include both inactive and active users, **True** to include only inactive users, or **False** to not include inactive users.

Identity Extended Attributes

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Table 43—Privileged User Access Report Identity Extended Attributes

Option	Description
Region	The user attributes on which to filter. Only users with the listed attributes are included in the report. This information is discovered during identity aggregation. **Note: Identity attributes are configurable and the attributes displayed might vary for each instance of the product.**
Department	The manager list to include in this report. Only users who report to the selected managers are included in the report. Click the arrow to the right of the suggestion field to display a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.
Location	The groups or populations to include in the report. Click the arrow to the right of the field and select **Populations**, to display a select list of populations, or select a group factory name to display a select list of groups created by that factory. Click on populations and groups from the select lists to create the inclusion list for this report. Click an item in the inclusion list to remove it from the report.
Employee ID	Select an operator from the list, Before or After, and specify a date manually or click the **"..."** icon and select one using the calendar options. Optionally include identities that have never been refresh.

Table 43—Privileged User Access Report Identity Extended Attributes

Option	Description
Job Title	Select an operator from the list, Before or After, and specify a date manually or click the **"..."** icon and select one using the calendar options. Optionally include identities that have never logged in to the product.
Region Owner	Specify that the report should include only active or only inactive identities.
Location Owner	The roles to include in the report. If no roles are specified, all roles are included. Click the arrow to the right of the suggestion field to display a list of all roles, or enter a few letters in the field to display a list of roles that start with that letter string.
DN	Specify a unique name for the Distinguished Name.
Cost Center	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Match Mode	Select the capabilities to include in the report.

Uncorrelated Accounts Report

The Uncorrelated Accounts Report includes information on all uncorrelated accounts that match the criteria specified.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Uncorrelated Accounts Report consists of the following sections:

- Standard Properties
- Uncorrelated Accounts Parameters
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Uncorrelated Accounts Parameters

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Note: Selecting NO options from a list indicates that ALL options in the list are included in the report.

Table 44—Uncorrelated Accounts Report Uncorrelated Accounts Parameters

Option	Description
Correlated Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string. Correlated Applications are applications that are to be compared with the authoritative application. Any identity that has an account on the correlated application but not on the authoritative application is considered uncorrelated.

User Account Attributes Report

The User Account Attributes Report includes information on all attributes for a given account on each application that match the criteria specified.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The User Account Attributes Report consists of the following sections:

- Standard Properties
- Account Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Account Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Note: **Selecting NO options from a list indicates that ALL options in the list are included in the report.**

Table 45—User Account Attributes Report Account Properties

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
User Inactive Status	Choose how the report handles inactive users. Select **Include All** to include both inactive and active users, **True** to include only inactive users, or **False** to not include inactive users.

User Account Authentication Question Status Report

The Account Authentication Question Status Report includes information about users with insufficient challenge questions.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Account Authentication Question Status Report consists of the following sections:
- Standard Properties
- Identity Attributes
- Identity Extended Attributes
- Additional Identity Details
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:
- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Identity Attributes

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Table 46— User Account Authentication Question Status Report Identity Attributes

Option	Description
First Name	Input the first name of the identity you wish the report to include. For example, if you input "John" in the field, the report includes information on identities whose first name is John.
Last Name	Input the last name of the identity you wish the report to include. For example, if you input "Smith" in the field, the report includes information on identities whose last name is Smith.
Display Name	Input the display name of the identity you wish the report to include. For example, if you input "John_Smith" in the field, the report includes information on identities whose display name is John_Smith.
Email	Input the email address of the identity you wish the report to include. For example, if you input "John@email.com" in the field, the report includes information on identities whose email address is name is John@email.com.
Manager	The manager list to include in this report. Only users who report to the selected managers are included in the report. Click the arrow to the right of the suggestion field to a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.
Inactive	Choose how the report handles inactive identities. Select **No selection** to include both inactive and active identities, **True** to include only inactive identities, or **False** to not include inactive identities.

Identity Extended Attributes

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Table 47—User Account Authentication Question Status Report Identity Extended Attributes

Option	Description
Region	The user attributes on which to filter. Only users with the listed attributes are included in the report. This information is discovered during identity aggregation. **Note: Identity attributes are configurable and the attributes displayed might vary for each instance of the product.**
Department	The manager list to include in this report. Only users who report to the selected managers are included in the report. Click the arrow to the right of the suggestion field to display a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.

Table 47—User Account Authentication Question Status Report Identity Extended Attributes

Option	Description
Location	The groups or populations to include in the report. Click the arrow to the right of the field and select **Populations**, to display a select list of populations, or select a group factory name to display a select list of groups created by that factory. Click on populations and groups from the select lists to create the inclusion list for this report. Click an item in the inclusion list to remove it from the report.
Employee ID	Select an operator from the list, Before or After, and specify a date manually or click the "**...**" icon and select one using the calendar options. Optionally include identities that have never been refresh.
Job Title	Select an operator from the list, Before or After, and specify a date manually or click the "**...**" icon and select one using the calendar options. Optionally include identities that have never logged in to the product.
Region Owner	Specify that the report should include only active or only inactive identities.
Location Owner	The roles to include in the report. If no roles are specified, all roles are included. Click the arrow to the right of the suggestion field to display a list of all roles, or enter a few letters in the field to display a list of roles that start with that letter string.
DN	Specify a unique name for the Distinguished Name.
Cost Center	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Match Mode	Select the capabilities to include in the report.

Additional Identity Details

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Table 48—User Account Authentication Question Status Report Additional Identity Details

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Capabilities	Select the capabilities to include in the report.
Roles	The roles to include in the report. Click the arrow to the right of the field and select a role to create the inclusion list for this report.

Table 48—User Account Authentication Question Status Report Additional Identity Details

Option	Description
Groups	The groups or populations to include in the report. Click the arrow to the right of the field and select a group to create the inclusion list for this report.
Last Refresh Date	Select a date range to filter users based on when the user was last refreshed.
Last Login Date	Select a date range to filter users based on when the user was last logged in.

User Details Report

The User Details Report includes information on user and their associated attributes. The report searches the identity cubes to extract the desired information.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The User Details Report consists of the following sections:

- Standard Properties
- Identity Attributes
- Identity Extended Attributes
- Additional Identity Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Identity Attributes

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Table 49— User Details Report Identity Attributes

Option	Description
First Name	Input the first name of the identity you wish the report to include. For example, if you input "John" in the field, the report includes information on identities whose first name is John.
Last Name	Input the last name of the identity you wish the report to include. For example, if you input "Smith" in the field, the report includes information on identities whose last name is Smith.
Display Name	Input the display name of the identity you wish the report to include. For example, if you input "John_Smith" in the field, the report includes information on identities whose display name is John_Smith.
Email	Input the email address of the identity you wish the report to include. For example, if you input "John@email.com" in the field, the report includes information on identities whose email address is name is John@email.com.
Manager	The manager list to include in this report. Only users who report to the selected managers are included in the report. Click the arrow to the right of the suggestion field to a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.
Inactive	Choose how the report handles inactive identities. Select **No selection** to include both inactive and active identities, **True** to include only inactive identities, or **False** to not include inactive identities.

Identity Extended Attributes

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Table 50—User Details Report Identity Extended Attributes

Option	Description
Region	The user attributes on which to filter. Only users with the listed attributes are included in the report. This information is discovered during identity aggregation. **Note: Identity attributes are configurable and the attributes displayed might vary for each instance of the product.**
Department	The manager list to include in this report. Only users who report to the selected managers are included in the report. Click the arrow to the right of the suggestion field to display a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.

Table 50—User Details Report Identity Extended Attributes

Option	Description
Location	The groups or populations to include in the report. Click the arrow to the right of the field and select **Populations**, to display a select list of populations, or select a group factory name to display a select list of groups created by that factory. Click on populations and groups from the select lists to create the inclusion list for this report. Click an item in the inclusion list to remove it from the report.
Employee ID	Select an operator from the list, Before or After, and specify a date manually or click the **"…"** icon and select one using the calendar options. Optionally include identities that have never been refresh.
Job Title	Select an operator from the list, Before or After, and specify a date manually or click the **"…"** icon and select one using the calendar options. Optionally include identities that have never logged in to the product.
Location Owner	The roles to include in the report. If no roles are specified, all roles are included. Click the arrow to the right of the suggestion field to display a list of all roles, or enter a few letters in the field to display a list of roles that start with that letter string.
Region Owner	Specify that the report should include only active or only inactive identities.
Cost Center	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Match Mode	Select the capabilities to include in the report.

Additional Identity Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Table 51—User Details Report Additional Identity Properties

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Capabilities	Select the capabilities to include in the report.
Roles	The roles to include in the report. Click the arrow to the right of the field and select a role to create the inclusion list for this report.
Groups	The groups or populations to include in the report. Click the arrow to the right of the field and select a group to create the inclusion list for this report.

Option	Description
Last Refresh Date	Select a date range to filter users based on when the user was last refreshed.
Last Login Date	Select a date range to filter users based on when the user was last logged in.

Users by Application Report

The Users by Application Detail Report includes a list of all users that have accounts on the specified applications.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Users by Application Detail Report consists of the following sections:

- Standard Properties
- Report Options
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Report Options

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Note: Selecting NO options from a list indicates that ALL options in the list are included in the report.

Table 52—Users by Application Detail Report Options

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.

Policy Enforcement Reports

Policy Violation Report

The Policy Violation Report includes policy violations and the information associated with them. Policy violations are defined for your enterprise during configuration.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Policy Violation Report consists of the following sections:
- Standard Properties
- Policy Violation Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:
- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Policy Violation Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Note: **Selecting NO options from a list indicates that ALL options in the list are included in the report.**

Table 53—Policy Violation Report Policy Violation Properties

Option	Description
Identities	Select the identities to include in the report. If no identities are specified, all identities are included. Click the arrow to the right of the suggestion field to display a list of all identities, or enter a few letters in the field to display a list of identities that start with that letter string. Only violations associated with the selected identities are included in the report.
Policy	The policies to include in this report. Only violations of the policies selected from the list are included in the report.

Option	Description
Violation Activity	Use the radio buttons to include only active violations, inactive violations or all violations in the report.
Violation Date	Only the violations discovered before this date are included in the report.
Violation Status	Use to filter the report by violation status type. Choose from Open Violations, Inactive Violations, and All Violations.

Risk Reports

Applications Risk Live Report

The Application Risk Live Report includes summary information on the risk associated with each application that matches the specified criteria and the accounts that contribute to that risk.

Summary reports include mainly charts, graphs and summary statistics that highlight status of different areas within IdentityIQ. These reports cannot be exported to the CSV format.

The Application Risk Live Report consists of the following sections:
- Standard Properties
- Report Options
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:
- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Report Options

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Note: **Selecting NO options from a list indicates that ALL options in the list are included in the report.**

Table 54—Application Risk Live Report Options

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Owners	The application owners to include in the report. Only applications associated with selected application owners are included in the report Click the arrow to the right of the suggestion field to display a list of all owners, or enter a few letters in the field to display a list of owners that start with that letter string.

Identity Risk Live Report

The Identity Risk Live Report includes information on the risk associated with each identity that matches the specified criteria.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Identity Risk Live Report consists of the following sections:

- Standard Properties
- Identity Attributes
- Identity Extended Attributes
- Additional Identity Details
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Identity Attributes

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Note: **Selecting NO options from a list indicates that ALL options in the list are included in the report.**

Note: **Use the Shift and Crtl keys to select multiple items from lists.**

Table 55—Identity Risk Live Report Identity Attributes Options

Option	Description
First Name	Input the first name of the identity you wish the report to include. For example, if you input "John" in the field, the report includes information on identities whose first name is John.
Last Name	Input the last name of the identity you wish the report to include. For example, if you input "Smith" in the field, the report includes information on identities whose last name is Smith.
Display Name	Input the display name of the identity you wish the report to include. For example, if you input "John_Smith" in the field, the report includes information on identities whose display name is John_Smith.
Email	Input the email address of the identity you wish the report to include. For example, if you input "John@email.com" in the field, the report includes information on identities whose email address is name is John@email.com.
Managers	The manager list to include in this report. Only users who report to the selected managers are included in the report. Click the arrow to the right of the suggestion field to a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.
Inactive	Choose how the report handles inactive users. Select **No selection** to include both inactive and active users, **True** to include only inactive users, or **False** to not include inactive users.

Identity Extended Attributes

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Note: **Selecting NO options from a list indicates that ALL options in the list are included in the report.**

Note: **Use the Shift and Crtl keys to select multiple items from lists.**

Table 56—Identity Risk Live Report Identity Extended Attributes Options

Option	Description
Region	The user attributes on which to filter. Only users with the listed attributes are included in the report. This information is discovered during identity aggregation. **Note: Identity attributes are configurable and the attributes displayed might vary for each instance of the product.**

Table 56—Identity Risk Live Report Identity Extended Attributes Options

Option	Description
Department	The manager list to include in this report. Only users who report to the selected managers are included in the report. Click the arrow to the right of the suggestion field to display a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.
Location	The groups or populations to include in the report. Click the arrow to the right of the field and select **Populations**, to display a select list of populations, or select a group factory name to display a select list of groups created by that factory. Click on populations and groups from the select lists to create the inclusion list for this report. Click an item in the inclusion list to remove it from the report.
Employee ID	Select an operator from the list, Before or After, and specify a date manually or click the **"..."** icon and select one using the calendar options. Optionally include identities that have never been refresh.
Job Title	Select an operator from the list, Before or After, and specify a date manually or click the **"..."** icon and select one using the calendar options. Optionally include identities that have never logged in to the product.
Location Owner	The roles to include in the report. If no roles are specified, all roles are included. Click the arrow to the right of the suggestion field to display a list of all roles, or enter a few letters in the field to display a list of roles that start with that letter string.
Region Owner	Specify that the report should include only active or only inactive identities.
Cost Center	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Match Mode	Select the capabilities to include in the report.

Additional Identity Details

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Note: **Selecting NO options from a list indicates that ALL options in the list are included in the report.**

Note: **Use the Shift and Crtl keys to select multiple items from lists.**

Table 57—Identity Risk Live Report Additional Identity Details

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.

Option	Description
Capabilities	Select the capabilities to include in the report.
Roles	The roles to include in the report. Click the arrow to the right of the field and select a role to create the inclusion list for this report.
Groups	The groups or populations to include in the report. Click the arrow to the right of the field and select a group to create the inclusion list for this report.
Last Refresh Date	Select a date range to filter users based on when the user was last refreshed.
Last login Date	Specify a login date range manually or click the calendar icon and select one using the calendar options.

Risky Accounts Report

The Risky Accounts Report includes information on risky accounts in your enterprise and the reasons associated with their risk.

Summary reports include mainly charts, graphs and summary statistics that highlight status of different areas within IdentityIQ. These reports cannot be exported to the CSV format.

The Risky Accounts Report consists of the following sections:

- Standard Properties
- Report Options
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Report Options

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Note: **Selecting NO options from a list indicates that ALL options in the list are included in the report.**

Table 58—Risky Accounts Report Options

Option	Description
Correlated Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string. Correlated Applications are applications that are to be compared with the authoritative application. Any identity that has an account on the correlated application but not on the authoritative application is considered uncorrelated.

Role Management Reports

Role analytics are an important part of the overall role life-cycle management. Role analytics provide role managers the ability to be proactive in their approach to monitoring and improving the role model within your organization. Role modeling is an iterative and constant process. As your business needs change, security features improve, and new applications and user are added to your enterprise, your role model will have to change accommodate them. Use role analytics to keep up with those changing needs and adjust your model as needed.

Identity Roles Report

The Identity Roles Report includes information on each role assigned to the identities specified by the report criteria.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Identity Roles Report consists of the following sections:

- Standard Properties
- Identity Attributes
- Identity Extended Attributes
- Additional Identity Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Identity Attributes

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> **Note:** **Selecting NO options from a list indicates that ALL options in the list are included in the report.**

> **Note:** **Use the Shift and Crtl keys to select multiple items from lists.**

Table 59—Identity Roles Report Identity Attributes Options

Option	Description
First Name	Input the first name of the identity you wish the report to include. For example, if you input "John" in the field, the report includes information on identities whose first name is John.
Last Name	Input the last name of the identity you wish the report to include. For example, if you input "Smith" in the field, the report includes information on identities whose last name is Smith.
Display Name	Input the display name of the identity you wish the report to include. For example, if you input "John_Smith" in the field, the report includes information on identities whose display name is John_Smith.
Email	Input the email address of the identity you wish the report to include. For example, if you input "John@email.com" in the field, the report includes information on identities whose email address is name is John@email.com.
Manager	The manager list to include in this report. Only users who report to the selected managers are included in the report. Click the arrow to the right of the suggestion field to a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.
Inactive	Choose how the report handles inactive users. Select **No selection** to include both inactive and active users, **True** to include only inactive users, or **False** to not include inactive users.

Identity Extended Attributes

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Note: Selecting NO options from a list indicates that ALL options in the list are included in the report.

Note: Use the Shift and Crtl keys to select multiple items from lists.

Table 60—Identity Roles Report Identity Extended Attributes Options

Option	Description
Region	The user attributes on which to filter. Only users with the listed attributes are included in the report. This information is discovered during identity aggregation. **Note: Identity attributes are configurable and the attributes displayed might vary for each instance of the product.**
Department	The manager list to include in this report. Only users who report to the selected managers are included in the report. Click the arrow to the right of the suggestion field to display a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.
Location	The groups or populations to include in the report. Click the arrow to the right of the field and select **Populations**, to display a select list of populations, or select a group factory name to display a select list of groups created by that factory. Click on populations and groups from the select lists to create the inclusion list for this report. Click an item in the inclusion list to remove it from the report.
Employee ID	Select an operator from the list, Before or After, and specify a date manually or click the **"..."** icon and select one using the calendar options. Optionally include identities that have never been refresh.
Job Title	Select an operator from the list, Before or After, and specify a date manually or click the **"..."** icon and select one using the calendar options. Optionally include identities that have never logged in to the product.
Location Owner	The roles to include in the report. If no roles are specified, all roles are included. Click the arrow to the right of the suggestion field to display a list of all roles, or enter a few letters in the field to display a list of roles that start with that letter string.
Region Owner	Specify that the report should include only active or only inactive identities.
Cost Center	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Match Mode	Select the capabilities to include in the report.

Additional Identity Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Note: Selecting NO options from a list indicates that ALL options in the list are included in the report.

Note: Use the Shift and Crtl keys to select multiple items from lists.

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Capabilities	Select the capabilities to include in the report.
Roles	The roles to include in the report. Click the arrow to the right of the field and select a role to create the inclusion list for this report.
Groups	The groups or populations to include in the report. Click the arrow to the right of the field and select a group to create the inclusion list for this report.
Last Refresh Date	Select a date range to filter users based on when the user was last refreshed.
Last Login Date	Select a date range to filter users based on when the user was last logged in.

Role Archive Report

The Role Archive Report includes information on each role configure in IdentityIQ that matches the specified criteria.

This report is an archive-type report. Archive reports include end-of-period and task information that is formatted for easy dissemination of key audit information. Due to the large amount of data that is generated, the best option is to export the report results to a .pdf file.

The Role Archive Report consists of the following sections:

- Standard Properties
- Role Report Options
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Role Report Options

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> **Note:** **Selecting NO options from a list indicates that ALL options in the list are included in the report.**

Table 62—Role Archive Report Options

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string. Only roles associated with the selected applications are included in this report.
Type	Select types of roles to include in the report.
Owners	The list of role owners to include in this report. If no role owners are specified, the roles for all owners are included. Click the arrow to the right of the suggestion field to display a list of all role owners, or enter a few letters in the field to display a list of role owners that start with that letter string.
Status	Include only active roles or only inactive roles in the report.

Role Change History Report

The Role Change History Report includes detailed information on roles that have recently been changed.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Role Change History Report consists of the following sections:
- Standard Properties
- Role Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:
- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Role Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> **Note:** Selecting NO options from a list indicates that ALL options in the list are included in the report.

Table 63—Role Change History Report Properties

Option	Description
Change Start and End Date(s)	Filter request based on request date: **Start Date** — all changes made on or after the selected date. **End Date** — all changes made on or before the selected date.
Role Status	Include only active roles or only inactive roles in the report.
Type	Select types of roles to include in the report.
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string. Only roles associated with the selected applications are included in this report.
Owners	The list of role owners to include in this report. If no role owners are specified, the roles for all owners are included. Click the arrow to the right of the suggestion field to display a list of all role owners, or enter a few letters in the field to display a list of role owners that start with that letter string.

Role Details Report

The Role Details Report includes information on each role configured in IdentityIQ that matches the specified criteria.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Role Details Report consists of the following sections:

- Standard Properties
- Role Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Report Criteria

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> **Note:** Selecting NO options from a list indicates that ALL options in the list are included in the report.

Table 64—Role Detail Report Role Properties Options

Option	Description
Role Status	Include only active roles or only inactive roles in the report.
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string. Only roles associated with the selected applications are included in this report.
Owners	The list of role owners to include in this report. If no role owners are specified, the roles for all owners are included. Click the arrow to the right of the suggestion field to display a list of all role owners, or enter a few letters in the field to display a list of role owners that start with that letter string.
Role Type	Select types of roles to include in the report.

Role Members Report

The Role Members Report includes information on the members of each role that match the specified criteria.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Role Members Report consists of the following sections:
- Standard Properties
- Role Options
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:
- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Certification Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> **Note:** Selecting NO options from a list indicates that ALL options in the list are included in the report.

Table 65—Role Members Report Certification Properties

Option	Description
Role Status	Include only active roles or only inactive roles in the report.
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Role Owners	To filter access reviews based on their tags, select one or more tags. If multiple tags are selected, only access reviews that match all selected tags are included in this report.
Type	Select types of roles to include in the report.
Empty Roles	Select from All Roles, Only EMpty Roles or Only Populated Roles

Role Profiles Composition Report

The Role Profiles Composition Report returns information on the entitlements that comprise each role that matches the specified criteria.

This report returns information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Role Profiles Composition Report consists of the following sections:

- Standard Properties
- Role Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see "Standard Report Properties" on page 193.

For more information on Report Layout, see "Report Layout" on page 194.

For step by step instruction on creating or editing a report, see "Working with Reports" on page 181.

Role Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Note: **Selecting NO options from a list indicates that ALL options in the list are included in the report.**

Table 66—Role Profiles Composition Report Properties

Option	Description
Role Status	Include only active roles or only inactive roles in the report.
Roles Without Profiles	Include only roles that contain no profiles or only roles that contain at least one profile.
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string. Only roles associated with the selected applications are included in this report.
Owners	The list of role owners to include in this report. If no role owners are specified, the roles for all owners are included. Click the arrow to the right of the suggestion field to display a list of all role owners, or enter a few letters in the field to display a list of role owners that start with that letter string.
Type	Select types of roles to include in the report.

Chapter 30: Managing Application and Identity Risk Scores

Use the Identity Risk Score page to view individual risk scores for users. The page displays one tab for each risk level defined in IdentityIQ. The risk criteria and number of risk levels are defined during the configuration process.

Use the Application Risk Scores page to view the risk scores associated with each application. This page displays a table that summarizes all of the applications score cards. The score information for each applications is separated into scoring components that were defined when the product was configured.

For detailed information on the risk score pages, see:

Identity Risk Scores

Use this page to view individual risk scores for users. The page displays one tab for each risk level defined in IdentityIQ. Click a tab to display a list of all of the users that fall into that risk level.

You can access this page from the navigation menu bar. Go to Intelligence -> Identity Risk Scores.

Use the filter options to reduce the number of identities displayed on the list. The **Group to filter by** drop-down list is contains all of the groups defined for your enterprise when IdentityIQ was configured and is based on attributes use for identity mapping. The **Value** drop-down list contains all of the values assigned to the selected attribute.

Identity risk scores are determined by weighted scores assigned to components that comprise the individual's identity cube. The identity risk scores table lists the component scores and enables you to identify the areas most at risk and take the appropriate actions.

From the Identity Risk Scores table you can schedule Identity Certifications for any or all identities listed. Identity Certifications are certification requests for identities with risk scores that warrant special attention. For example, a contract database administrator might require more frequent certification than a full-time employee. These do not replace the regularly scheduled certification requests, neither Manager nor Application, but are in addition to those certifications.

This page has the following information:

Table 1—Identity Risk Scores Column Descriptions

Column Name	Description
Identity selection box	Activate this check-box to mark this user as one for whom to request an Identity Certification.
Name	The login name of the user. Only users with risk scores that fall into the risk band associated with the selected tab are displayed.
First Name	The first and last name of the user.
Last Name	

Column Name	Description
Composite Score	The total composite risk score for the user. This score is based on risk factors defined when IdentityIQ was configured for your enterprise.
Role	The sum of compensated role risk scores as defined when IdentityIQ was configured.
Entitlement	The sum of compensated entitlement scores as defined when IdentityIQ was configured.
Policy	The sum of compensated risk scores associated with policy violations as defined when IdentityIQ was configured.
Certification	The sum of compensated risk scores associated with certifications as defined when IdentityIQ was configured.

Click a user in the table to display the View Identity page. The View Identity page contains individual identity cube risk information. Identity Cubes are multi-dimensional data models of identity information that offer a single, logical representation of each managed user. Each Cube contains information about user entitlements, associated context and historical records of user access configurations and activity.

Application Risk Scores

Use this page to view the risk scores associated with each application. This page displays a table summarizing all of the applications score cards. The score information for each applications is broken down by the scoring components defined when the product was configured. The first column in the table contains the composite risk score for the application. The composite score is calculated by combining the compensated scores of the individual components.

Click an application in the table to display the Edit Application page. Click the **Risk** tab to view the latest score card for the application.

You can access this page from the navigation menu bar. Go to **Intelligence -> Application Risk Scores**.

The algorithms used by the Refresh Application Scoring task to update this page are defined on the Application Risk page.

All scores are calculated by first determining the percentage of accounts that have the qualities tested by the component score. For example, if 10 out of 100 accounts are flagged as service accounts, then the raw percentage is ten percent (.10). This number is then multiplied by a sensitivity value which can be used to increase or decrease the impact of the original percentage. The default sensitivity value is 5 making the adjusted percentage fifty percent (.50). This final percentage is then applied to the score range of 1000 resulting in a component score of 500.

After the component score is calculated, a weight or compensating factor is applied to each component score to determine the amount each will contribute to the overall risk score for the application. For example, a few violator accounts might increase risk more than many inactive accounts.

Service, Inactive, and Privileged component scores look for links that have a configured attribute. For example, the component `service` with a configured value `true`.

The Dormant Account score looks for a configured attribute that is expected to have a date value, for example `lastLogin`. This algorithm has an argument, `daysTillDormant`, that defaults to thirty (30). If the last login

date is more than thirty (30) days prior to the current date, the account is considered dormant and is factored into the risk score.

The Risky Account score looks for links whose owning identity has a composite risk score greater than a configured threshold. The default threshold is five hundred (500).

The Violator Account score looks for links whose owning identity has a number of policy violations greater than a a configured threshold. The default threshold is ten (10).

-

Section IV Lifecycle Manager

Use the following components to work with SailPoint's Lifecycle Manager.

Chapter 31: Lifecycle Manager Overview

IdentityIQ Lifecycle Manager manages changes to user access and automates provisioning activities in your enterprise environment. The Lifecycle Manager maps directly to the lifecycle of a user in an organization and the core identity business processes associated with the user lifecycle activities (joining, moving, leaving).

- User Lifecycle Activities — joining, moving, leaving
- Core Identity Processes — provision, change, de-provision

The Lifecycle Manager can be configured to enable users to make requests through IdentityIQ and control which requests they can make.

Users

- Individual User — can make requests using the self-service feature
- Managers — can make requests for direct reports
- Help Desk Operators — can make requests for populations
- Other users — controls requests by all users not a part of the standard groups

User Requests

- New access — request entitlement and roles
- Account Management— create, manage, and delete accounts including enable, disable, and unlock, change and reset passwords, and track current requests
- Identity Management — create, edit, and view identities

Automated Change Management Using Configurable Event Triggers

Lifecycle Manager provides automated change management based on configurable identity lifecycle event triggers. These triggers are mapped to different identity-related events in an authoritative source, typically an human resources system. When a tracked event is detected, provisioning requests are generated. For example, when the status of an employee changes from active to terminated, this lifecycle event can be configured to trigger a de-provisioning request for all of the access associate with the employee. If an employee's job title changes, a trigger can launch the assignment of a new business role to replace the employee's current business role.

IdentityIQ **Governance Platform**

Lifecycle Manager leverages the IdentityIQ Governance Platform to enhance compliance performance, improve security, and reduce risk.

SailPoint uses a combination of roles, policy, and risk to provide a framework for evaluating all requests for changes to access against predefined business policies.

- IdentityIQ **Role Model —** simplifies administration of user access by providing a predefined and planned structure for requesting and validating user access based on business or IT roles.
- IdentityIQ **Policy Model —** evaluates your corporate access policies during the access request and provisioning processes.
- IdentityIQ **Risk Model —** reduces operational risk by using a risk-based approach to identity governance and provisioning by enabling organizations to modify change management processes.

Identity Broker

Lifecycle Manager uses the IdentityIQ Provisioning Broker to manage the final change manage activities that are the result of self-service access requests or automated lifecycle event triggers. The IdentityIQ Provisioning Broker is a key piece of the IdentityIQ architecture that enables organizations to coordinate changes to user access across different provisioning processes. When a provisioning change is triggered, the provisioning broker separates each request into its component parts and determines the appropriate provisioning implementation process. Provisioning options include:

- The SailPoint Automated Change Manager
- 3rd-party user provisioning solutions, such as Oracle IdM
- Service request systems, such as BMC Remedy
- Email generated to a system administrator

Chapter 32: Lifecycle Manager Components

Lifecycle Manager is a part of your IdentityIQ solution that adds tools, work items and reports related to Lifecycle Manager core functionality.

New User Registration — a self-service feature that enables new users to request initial access to IdentityIQ. When access is granted, a new identity cube is created for the user.

Quicklink Cards — convenient links to request and track user access from your Home page.

How to Manage Access

Lifecycle Manager adds Manage Access links to Home page. Use the links to perform the following functions:

> **Note:** **IdentityIQ System Administrators can make any request regardless of the Lifecycle Manager Configuration settings.**

Requests are processed based on the business process defined when IdentityIQ is configured for your organization. If approval is not required, the roles are added or removed from the entitlements list and are available after the associated access is granted on the required applications. If approval is required, the request must first pass the approval process before being assigned.

Requests can be processed:
- Manually
- Through a work item
- By generating a help ticket, if your implementation is configured to work with a help desk solution
- Automatically through a provisioning provider

-

Request Violations

> **Note:** **The section only applies for single identity access requests. If a request for multiple users contains violations, the request goes through and notifications are sent.**

When you submit an access request that results in a policy violation and IdentityIQ is configured to have interactive violation handling, a warning message appears at the top of the page with a list of the violations. Click a violation to view details about the violation possibly including compensating controls and correction advice if they were included.

Access Request Violations Options

For access requests that generate policy violations, IdentityIQ can be configured to:
- "Reject and Cancel Requests with Policy Violations" on page 276
- "Allow Requests with Policy Violations - Non-Interactive" on page 276
- "Reject Requests with Policy Violations - Interactive" on page 276
- "Allow Requests with Policy Violations - Interactive" on page 277

Reject and Cancel Requests with Policy Violations

If you submit an access request that results in a policy violation and IdentityIQ is configured to reject any requests with policy violations, the request fails and is canceled. You can navigate to the Manage Use Access page and create a new request.

Reject Requests with Policy Violations - Interactive

If you submit an access request that results in a policy violation and IdentityIQ is configured to reject any requests with policy violations, the request fails. If you are notified that the request failed because of a policy violation, and you are still on the Manage User Access page, you can:
- Change the access request
- Cancel the access request

Allow Requests with Policy Violations - Non-Interactive

If you submit an access request that results in a policy violation and IdentityIQ is configured to allow any requests with policy violations, the request goes through and you are not notified.

Allow Requests with Policy Violations - Interactive

If you submit an access request that results in a policy violation and IdentityIQ is configured to allow requests with policy violations, and notify the requester, the request continues. When you are notified of the violation, you can:

- Change the access request
- Cancel the access request
- Continue with the access request

> **Note:** **When you continue with an access request with a violation, IdentityIQ can be configured to allow the violation with no user interaction or require users to add a comment or sunset date.**

Manage Accounts

> **Note:** **The status for the accounts listed on the Manage Accounts page are refreshed automatically based on the conditions set during configuration.**

You can use the **Manage Accounts** link to take action on any of the accounts assigned to a user. Based on how you system is configured, you can:

- View account information
- Delete and account
- Disable/Enable an account
- Refresh account status
- Request an account

Manage Accounts Page

The Manage Accounts page displays the user's cards that you can manage. From this page, you can:

- **Search** for a user — Enter a letter or combination of letters and click the **Search** icon.
- **Manage** a user's accounts — Select a user's card and click **Manage**.

The Accounts section lists information about accounts associated with the selected user. Information can include:

Table 1—Manage Accounts Column Descriptions

Column Name	Description
Application	The application specific to the Account ID.
Account ID	Name of the account.
Status	The current status of the account.
Application	The application specific to the Account ID.
Last Refresh	The date the account information in IdentityIQ was last updated.
Last Action Status	The status of the last provisioning operation performed though IdentityIQ. This state is not updated by actions performed outside of IdentityIQ, so might not reflect the current state of the account.

The available actions are represented by icons defined in the legend on the page. Click an icon to perform the specified action.

> **Note:** **If the application does not support the action, the icon is not visible. These options are only available if configured by an administrator.**

Click the **Refresh** icon to refresh the account status.

Click the **Information** icon to view information about the account.

Click the **Actions Menu** icon to perform available actions.

To request a new account for an application, click **Request Account** and select the application from the **Application** drop-down list.

-

Account Passwords

The Account Passwords link has the following options:

- Change — change a specific password or generate a new password for one or more accounts.
- Sync — synchronize a group of passwords.
- Generate — generate a single password for all selected accounts or generate a unique password for each selected account.
- Information icon — View details about the selected application.

> **Note:** **If you click the Home button, exit the IdentityIQ application, or navigate away from the manage access pages before you complete all tasks, your entries are cleared and the access request is NOT submitted.**

Account Password Tasks

Based on how your system is configured, the following tasks can be available:

- "Change a Password for a Single Application" on page 278
- "Use Synchronize to Set up a Single Password for Multiple Applications" on page 279
- "Use Generate to Manage a Group of Passwords" on page 279

Change a Password for a Single Application

To change an account password:

1. Navigate to the **Manage Passwords** page.

2. Select a user card and click **Manage.**

3. From the application list, navigate to the row for the application with the password you want to change and click **Change**.

4. In the row below the listing: you can:

   - Manually enter a new password, re-enter the password to confirm, and click **Submit**.

   - Or you can click **Generate** to generate a new password for the account.

> **Note:** **If there are any errors associated with the manually submitted password the text fields are highlighted in red. Information is displayed below the text field that describes why the submitted password failed and the password policy.**

Use Synchronize to Set up a Single Password for Multiple Applications

You cannot synchronize passwords for accounts with incompatible password policies. The Synchronize Password option is not available for self service accounts. To set up a single password for a group of applications:

1. Navigate to the **Manage Passwords** page.

2. Select a user card and click **Manage.**

3. From the account list, select the accounts.

4. In the Synchronize Passwords dialog, enter the new password.

5. Re-enter the new password to confirm and click **Confirm**.

Use Generate to Manage a Group of Passwords

To generate passwords for a group of applications:

1. Navigate to the **Manage Passwords** page.

2. Select a user card and click **Manage.**

3. From the account list, select the accounts.

4. In the Generate Passwords dialog, select:

    -   **Sync Password for All** to generate a new single password for all the selected accounts.

    -   Or **Generate Password for All** to generate a new password for all the selected accounts.

Track My Requests

To track the progress of access requests you created, click **Manage Access -> Track My Access Requests**, use the **Track My Access Requests** link on your Home page, or **My Work -> Access Requests** to display the Access Request page.

Click on a item in the list to display detailed information about the requested items and any pending actions that still need to be taken on that request.

From the detailed history panel you can navigate further into the request to expand the details view, review the actual access request, and send messages to owners of the request reminding them that their action is required.

Click the **X** icon to cancel a request.

Table 2—Access Requests Column Descriptions

Column Name	Description
Access Request ID	Identification number assigned to the access request.
Priority	Specifies the priority level to which the access request was designated.
Type	The type of access request.
Description	The a brief description of the access request.
Requester	The name of the user who assigned this work item to you.
Requestee	The name of the user to who was assigned this access request.

Table 2—Access Requests Column Descriptions

Column Name	Description
Request Date	The date the request was made.
Current Step	Status of the request. Status levels include: Pending — Request was received but no action has taken place. Approved — Request was approved. Additional action may be needed to complete the request. Rejected — Request was denied. Completed — All actions required for this access request have been fulfilled. Cancelled — Request was cancelled. Completed Pending Verification — The manual action for this request was completed, however the verification procedure has yet to have been run.
Completion Date	The date when the work item was completed.
Execution Status	Status of the request execution. Status levels include: Executing — The request is going through the business process and has not completed. Verifying — The request has finished the business process and is waiting for the Provisioning Scanner to verify it. Terminated — The request was terminated before it was completed. Completed — The request was completed and verified.

Access Requests Page

The Access Requests page provides a central location that lists Access Requests and an overview of information about each request. To search for an access request, enter an Identity in the search box and click the search icon. For use additional search criteria, click **Advanced Search**.

Click an access request listing to view the following information about an access request:

- **Request Items** — displays details about the Operation, Item, Value, Account, application, Instance, Comments, Approval Status and Provisioning Status for the selected access request. To view all available details for an access request, Click **View Complete Details**.

- **Pending Interactions** — displays the Description, Owner, Open Date and Details for any access request that is not complete. To send an email to an owner, click the **email icon** next to the name of the owner.

  Note: **If your administrator set up a template for an email reminder, a pre-populated email is displayed. If a template was not set up, an empty email form is displayed and you are prompted to provide the required subject and body fields.**

How to Manage Identities

Based on the IdentityIQ configuration, the following options can be available:

- "Create Identity" on page 281
- "Edit Identity" on page 281
- "View Identity" on page 281

Create Identity

To create new identity cubes in IdentityIQ, use the Create Identity page. The data fields are based on the fields defined as standard and/or searchable attributes in the IdentityIQ configuration.

Click Submit after all selections are completed.

-

Edit Identity

Use the Edit Identity page to edit identity attributes in IdentityIQ. The data fields are based on the fields defined as standard or searchable attributes in the IdentityIQ configuration.

Select an identity from the Available Identities list to display the Edit Identity Attributes page.

Use the search and filter features to limit the number of identities displayed.

Click **Submit** after all selections are completed to display the Review and Submit page.

-

View Identity

Use the View Identity page to view detailed information about an identity in IdentityIQ. This page can be accessed from the **Define -> Identities** page.

Select an identity from the Available Identities list to display the View Identity page.

Use the search and filter features to limit the number of identities displayed.

See, "Identity Details Page" on page 128.

●

Identity Details Menu

Based on the IdentityIQ configuration, the following options can be available:

- **Edit** — allows you to edit identity details.
- **Forward** — allows you to assign a user for forwarding.
- **Attributes** — lists the basic user identity information such as first name, last name, and email, as well as enabling you to update the user password and the forwarding user.
- **Access** — lists all of the user's roles and entitlements.
- **Accounts** — lists account information for all of the applications to which the user has some level of access.
- **Account Passwords** — allow you to manage account passwords for one or more applications.
- **System Password** — allows you to manage IdentityIQ system passwords.

Lifecycle Manager Optional Links

The following items are optional Lifecycle Manager links that your administrator can configure:

- Manage Recycle Bin — provides support for deleted users, groups with all their attributes, and group memberships.
- Update My RSA Token PIN — provides support for updating you RSA Token PIN. See

How to Update My RSA Token PIN

Note: If you are logged in and have an RSA link associated with your identity, the Update My RSA Token PIN option is available.

- To reset a PIN, click the **Update My RSA Token PIN** link on the Lifecycle Manager. The form displays the serial numbers of the tokens assigned to you. Select one of the multiple tokens (serial numbers) and type in a new PIN. The PIN is reset and changed in the target system. If you have multiple tokens and want to modify the PIN for all of the token, you must make a separate request for each token.

Chapter 33: Manage User Access

IdentityIQ can be set up to request and manage access for yourself or for other identities. Based on how your system is configured, you can manage:

- "Access for Others" on page 283 — Users request and manage access for one or more identities. This option can also be set up to enable you to request access for yourself.
- "Access for Yourself" on page 283 — Users request and manage access for themselves.

    Note: **If you click the Home button, exit the IdentityIQ application, or navigate away from the manage access pages before you complete all tasks, your entries are cleared and the access request is NOT submitted.**

Access for Others

The following tabs are displayed for systems that are configured to request and manage access for one or more users:

- **Select Users** — Displays a list of available identities. You can choose one or more identities from the list.
- **Manage Access** — Use **Search** or **Filter** to find available roles and entitlements, or click **Browse all access** to display all available roles and entitlements. You can select **Add Access** to add new access. Select **Remove Access** to remove access for a single user.

    Note: **When removing access, only the roles and entitlements the user has will be available to remove.**
- **Review and Submit** — Displays access request information. You can verify and submit your access requests.

Access for Yourself

The following tabs are displayed for systems that are configured to request and manage access for a single identity:

- **Manage My Access** — Use **Search** or **Filter** to find available roles and entitlements, or click **Browse all access** to display all available roles and entitlements. Click the check icon for each access item you want to add. You can also click **Remove Access** to see the access you currently have and select access you want to remove.
- **Review and Submit** — Displays your access request information. You can verify and submit your access requests.

Selecting and Deselecting Items

Click the check icon associated with the listing to select an item. Click **All** to select all displayed items. To deselect an item, click the highlighted check icon associated with the listing. If you do not want a selected user or an access item to be included in your access request, you must deselect it. Click **Home** to clear all items and cancel a request.

Request Access Tasks

Based on how your system is configured, you can perform the following tasks:

Request Access

Based on how your system is configured, you can:

Request Access for Others

This option must be configured on the Lifecycle Manager configuration page.

1. On the **Select User** tab, click the check icon next on the card for one or more identities.
   To search for an identity, enter the name or first few letters of an identity in the search box and click the search icon. To limit the number of listings, click Filters, select specific filter criteria, and then click Apply

2. Navigate to the **Manage Access** tab and select the **Add Access** tab.
   To search, enter a term in the search box and click the search icon. Click the menu icon next to the search file to change between search types: Keyword, User Access, or Populations. To limit the number of listings, click Filters, select specific filter criteria, and than click Apply.

   Click **Browse all access items** to display the full list of access options available.

3. If a role or entitlement requires an account the identity does not have, the **Select Account** dialog displays. To create the new account, select the account and **click Apply**.

4. After IdentityIQ validates that the user does not currently have the requested access, the number of items you selected displays on the **Add Access** tab.

5. Navigate to the **Review and Submit** tab and review the access request information for each identity.

6. Before you complete the access request, you can:

   - Remove an access request entry — Click the **X** icon next to the access item.

   - Add an attachment (single user requests only) — See "Add Attachments" on page 287

   - Add a comment — See "View and Post Comments" on page 288.

   - Change the priority — See "Change Priority" on page 288.

   - Change the sunrise/sunset dates — See "Change Sunrise/Sunset Date" on page 289.

   Note: **After you click Submit, forms are issued if further information is needed before your request can be completed.**

   If you are requesting access for a single identity, a popup is displayed enabling you to complete the form immediately or send it to your Home page.

   If you are requesting access for multiple identities, the forms are sent directly to your Home page and no popup is displayed.

7. When you have completed all your review tasks, click **Submit** to complete the access request.

Request Access for Yourself

If your system is set up to allow you to request access for yourself, a card with your identity details is the first card displayed on the Select User tab. This option must be configured in IdentityIQ.

1. On the **Manage My Access** tab, select the **Add Access** tab.
   To search, enter a term in the search box and click the search icon. To limit the number of listings, click Filters, select specific filter criteria, then click Apply.

   Click **Browse all access items** to display the full list of access options available.

2. Some roles allow related roles to be added. To add the additional roles, select the role or roles and click **Continue**.

3. Navigate to the **Review and Submit** tab and review the access request information.

4. Based on how your system is configured, you can:

   - Remove an access request entry — Click the **X** icon next to the access item.

   - Add an attachment — See "Add Attachments" on page 287

   - Add a comment — See "View and Post Comments" on page 288.

   - Change the priority — See "Change Priority" on page 288.

   - Change sunrise and sunset dates — See "Change Sunrise/Sunset Date" on page 289.

5. When you have completed all your review tasks, click **Submit** to complete the access request.

Request Access Containing a Permitted Role

A permitted role is generally a requested or assigned role and is not automatically granted to a user. Permitted roles are enabled by default. When permitted roles are available, they are displayed on the following tabs:

- **Add Access** — When you select a role that has permits, the associated permitted roles are displayed as cards after you complete the account selection setup.
- **Review** — Permitted roles are displayed below the associated assigned role.

Note: You can set Sunrise/Sunset dates and comments on permitted roles.

Remove Access

The remove access feature is only available for an individual user.

Note: **If your system is set up to allow you to add or remove access for yourself, a card with your identity details is the first card displayed on the Select User tab.**

1.   On the **Select User** tab, click the arrow on the card for an identity.

2.   Navigate to the **Manage Access** tab and select the **Remove Access** tab. The current access for the selected user is displayed.
    To search, enter a term in the search box and click the search icon. To limit the number of listings, click Filters, select specific filter criteria, and than click Apply. Search in the Remove Access area includes a Status filter that allows you to filter results for Active or Requested access.

3.   Click the check icon next to the access items you want to remove. The number of items you selected to be deleted is displayed in a circle on the **Remove Access** tab.

4.   Navigate to the **Review and Submit** tab and review the information about the access you want to remove for the individual user.

5.   Before you complete the access actions, you can:

    -    Remove an access request entry — Click the **X** icon next to the access item.

    -    Add an attachment — See "Add Attachments" on page 287

    -    Add a comment — See "View and Post Comments" on page 288.

    -    View Details — See "View Details" on page 286.

6.   When you have completed all your review tasks, click **Submit**.

View Details

You can view the following information about a user:
- "View User Details" on page 286.
- "View Role Details" on page 286.

View User Details

Based on how your system is configured, you can view items such as User Name, Last Name, First, email, Location Owner, Region, and more.

1.   Navigate to the **Manage User Access** page.

2.   On the **Select User** tab, click the user icon on any user card.

To view user details from the Review tab, click the user name next to the user icon to return to the Select User tab and than click the user icon on the user card.

View Role Details

For any role, you can view information such as the application associated with the role, the Attribute, the Name of the role and how the role was assigned.

1. Navigate to the **Manage User Access** page.

2. On the **Manage Access** tab, click **Details** for any role listing.

Add Attachments

> Note: **IdentityIQ does not perform file content validation or verification on attachments. It is your responsibility to ensure that only files that do not violate security policies within your environment are included as attachments.**

> Note: **Attachments are only available for single user access requests. If attachments are enabled, you will see the attachment icon on all request items, but it will only be active on requests that support attachments.**

You can add attachments to access request items using the attachments button, paper clip icon. The number next to the icon indicates the number of files attached to that access request item. Based on how your system is configured, you can have the ability to add attachments, for example a training certificate or notarized document of authorization, or you might be required to add an attachment for specific items.

> Note: **If attachments are required, it will be indicated in the icon and you will receive a warning if you try to submit the request with out an attachment.**

> Note: **If attachments are required for an item and you include that item in a request for multiple users, a message is displayed instructing you to amend the request as required.**

> Note: **Adding any attachment will fulfill the required attachment rules. IdentityIQ does not validate to ensure the correct item was attached.**

1. On the **Review and Submit** tab, select the attachments icon for the request item.

2. In the attachments overlay, add attachments by dragging and dropping or uploading files.

3. Click **OK** after all files are loaded.

Attachment Overlay

The information displayed on the attachment overlay is controlled using AttachmentConfig rules. Every time a user accesses the **Review and Submit** tab of an access request, every AttachmentConfig rule is reviewed and the attachment overlay is constructed based on that input, possibly with the names of required or suggested attachments displayed in a list.

Required attachment names are display with a red asterisk. All required attachments should be included in the access request, but any attachment will satisfy the requirement rules. IdentityIQ does not validate the attached files.

Drag and drop or upload the attachments to add them to the **Attached to This Item** list.

The **Attached to This Item** list contains any files already attached to this request item. From this list you can:
- Add or edit comments — click the pencil icon to add or edit comments
- Download and view — download and view the attachment
- Remove — remove the attachment from the request and delete it from the database

View and Post Comments

You can view or post comments and assignment notes to an access request using the comments button, talk bubble icon. The number next to the icon indicates the number of comments and notes for the access request. Based on how your system is configured, you can:

- "View or Post Access Request Line Item Comments" on page 288.
- "Post an Assignment Note to Access Request Line Items" on page 288.

When you add a comment or assignment note to an access request line item, the note icon turns green.

> **Note:** Assignment notes can only be added to assigned roles. You cannot add assignment notes to permitted roles.

View or Post Access Request Line Item Comments

Before you complete and access request, you can view or post a comment to line items for entitlements and roles.

> **Note:** If an Assignment note is not permitted for the item, the title of the dialog is Comment.

1. On the **Review and Submit** tab, select the comments icon for the request item.

2. In the **Comments and Notes** dialog, select the **Comments** tab.

3. To post a new comment, type your comments in the text box and click **Save**.

Post an Assignment Note to Access Request Line Items

Before you complete an access request, you can post an assignment note to line items for roles.

> **Note:** If an assignment note is not permitted for the item, the Assignment Notes tab is not displayed.

1. On the **Review and Submit** tab, select the comments icon for the request item.

2. In the **Comments and Notes** dialog, select the **Assignment Notes** tab.

3. Type your note in the text box and click **Save**.

Edit an Access Request

Before you submit an Access Request, you make the following edits from the **Review and Submit** tab:

- "Change Priority" on page 288.
- "Change Sunrise/Sunset Date" on page 289.

Change Priority

> **Note:** For this feature to be available to users, the Administrator must enable the option to Allow requesters to set request priorities.

If your system is set up to allow priorities for access requests, you can change the priority for an access request. The default setting is **Normal Priority**. When you create an access request, you can change the priority to **High Priority** or **Low Priority.**

Before you complete an access request, you can change the priority for an access request:

1. On the **Review** tab, click the button with the flag icon.

2. Select **High Priority**, **Normal Priority**, or **Low Priority**.

Change Sunrise/Sunset Date

Sunrise and sunset dates support the temporary assignment of roles and entitlements by letting you set a beginning (sunrise) and an end (sunset) date for access. Access is deprovisioned when the sunset date arrives.

> **Note:** **For this feature to be available to users, the administrator must enable the option to allow Sunrise/Sunset dates on role assignment.**

> **Note:** **If you specify a global Sunrise/Sunset date on an entire access request, and than change the global setting, the new global setting overrides any individual line item date settings you made.**

Before you complete an access request, you can set a beginning and ending date for an:

- Individual line items in an access request — Any line item in the requests can be set to a date.
- Entire access request — Each line item in the request is set to the same date value even if there was no previous value.

If all the dates in access request are the same, the global date icon is green. If the dates for one or more line items in the access request are difference, the date icon is gray.

To set the global sunrise/sunset dates for a line items in an access request:

1. On the **Review** tab, click the date icon for the line item in the access request.

2. In the Set Sunrise/Sunset dates dialog, type a new date in the field in the mm/dd/yyyy format or click the calendar to select a date.

3. Click **Save** to save the new dates.

To set the global sunrise/sunset dates for an access request:

1. On the **Review** tab, click the date icon for the access request.

2. In the Set Sunrise/Sunset dates dialog, type a new date in the field in the mm/dd/yyyy format or click the calendar to select a date.

3. Click **Save** to save the new dates.

Request Violations

> **Note:** **The section only applies for single identity access requests. If a request for multiple users contains violations, the request goes through and notifications are sent.**

When you submit an access request that results in a policy violation and IdentityIQ is configured to have interactive violation handling, a warning message appears at the top of the page with a list of the violations. Click a violation to view details about the violation possibly including compensating controls and correction advice if they were included.

Access Request Violations Options

For access requests that generate policy violations, IdentityIQ can be configured to:

- "Reject and Cancel Requests with Policy Violations" on page 290
- "Allow Requests with Policy Violations - Non-Interactive" on page 290
- "Reject Requests with Policy Violations - Interactive" on page 290
- "Allow Requests with Policy Violations - Interactive" on page 290

Reject and Cancel Requests with Policy Violations

If you submit an access request that results in a policy violation and IdentityIQ is configured to reject any requests with policy violations, the request fails and is canceled. You can navigate to the Manage Use Access page and create a new request.

Reject Requests with Policy Violations - Interactive

If you submit an access request that results in a policy violation and IdentityIQ is configured to reject any requests with policy violations, the request fails. If you are notified that the request failed because of a policy violation, and you are still on the Manage User Access page, you can:

- Change the access request
- Cancel the access request

Allow Requests with Policy Violations - Non-Interactive

If you submit an access request that results in a policy violation and IdentityIQ is configured to allow any requests with policy violations, the request goes through and you are not notified.

Allow Requests with Policy Violations - Interactive

If you submit an access request that results in a policy violation and IdentityIQ is configured to allow requests with policy violations, and notify the requester, the request continues. When you are notified of the violation, you can:

- Change the access request
- Cancel the access request
- Continue with the access request

> **Note:** When you continue with an access request with a violation, IdentityIQ can be configured to allow the violation with no user interaction or require users to add a comment or sunset date.

Chapter 34: Approve Access Requests

Use the Approve Access Requests interface to make decisions on access request approvals that are assigned to you. If you are a member of any workgroups, the listings include approvals for those workgroups.

Click the **Approve Access Requests** Quicklink card or select **Approve Access Requests** in the Quicklink menu to access the Approvals page, which shows the access request approvals that are assigned to you. Use this page to view and manage your approval requests. Approval items include the following types of Lifecycle Manager access requests:

- Role Requests
- Entitlement Requests
- Account Requests

Approval items are shown in an expanded view by default, showing full details for all items in the request. Click **Collapse All** to switch to a more compact display showing only the approval-level details, without item details. Click **Expand All** to expand the listing to the detailed view.

To sort the list, click the arrow next to **Sort By** and select a sort type, **Newest**, **Oldest**, or **Priority**.

Use the **Filter** icon to filter the items that are displayed on the page. You can filter by **Owner**, **Requester**, or **Assignee**. When you have selected your filtering criteria, click **Apply**. When filtering is applied, the **Filter** icon turns green to alert you that you are seeing a filtered subset of your items. To clear filtering criteria and return to viewing all items, click **Filter** again, and click **Clear** to remove your filter criteria.

Use **Collapse All** or **Expand All** to control how the items are displayed.

Use the **Search** field to search for approval items by **Work Item ID** or **Requestee Name**.

Click **Recommendations** to display the Decision Recommendation popup. The recommendations icon is only displayed If SailPoint IdentityAI was purchased and activated for your installation of IdentityIQ. See the SailPoint *IdentityAI Implementation Guide* for more information.

Approval Tasks

You can perform the following tasks:

- "Complete an Approval" on page 291
- "Forward an Approval" on page 292
- "View Details" on page 292
- "View and Post Comments" on page 293
- "Edit an Approval" on page 8

Complete an Approval

> Note: **A Policy Violation alert is displayed at the top of any approval that causes a violation if the request is approved.**

You can take approval actions both at the overall approval request level, or at the individual request item level.

If SailPoint IdentityAI was purchased and activated for your installation of IdentityIQ, recommendation icons are displayed with each item for which a recommendation is available. Click the icon to see the recommendation details. See the SailPoint *IdentityAI Implementation Guide* for more information.

For each approval request you can:

- **Approve All** items, **Deny All** items, or **Forward** the approval.
- Make a decision on each individual approval item to **Approve** or **Deny** the request.
- Use an electronic signature to sign an approval if your installation is configured to use this feature.

> **Note:** **If the approval request was set up to use electronic signature, the Electronic Signature dialog displays automatically. Use the same credentials you use to sign in to the product.**

The Complete Approval dialog displays when you click **Approve All** or **Deny All** for an approval, or after you click the **Approve** or **Deny** button for the last individual item in an approval. To complete the approval, click **Complete**. To change your approval decisions, click **Cancel**.

Forward an Approval

You can forward an approval to another identity or workgroup, to pass the responsibility for approval decisions to them. Forwarded approvals can not be recalled, and once you forward an approval, you can no longer view informatoin about it. To forward an approval:

1. Click the **Forward** icon in the Actions (three-line) menu for an approval.

2. Enter the name or a few letters of the name of the new owner of the approval. Alternatively, you can click the down icon and select a name from the list.

3. Add any forwarding comments and click **Forward**.

View Details

You can view detailed information about an approval, its forwarding history, and information about any approval line item.

> **Note:** **For small form factors such a mobile phones, the Details button is displayed in the Actions menu.**

You can view the following types of details:
- "View Approval Details" on page 292
- "View Approval Line Item Details" on page 293

View Approval Details

Click the **Info** button for the overall approval to open the Details dialog. It shows the following items.

- **Work Item Details** tab— displays the work item and Access Request ID number, who made the request, who owns the approval, when the approval was created and the priority.
- **Identity Details** tab — displays the attributes that the Administrator configures for the Identity Mappings and can include attributes such as user name, first and last name for the identity, the email for the identity and the owner of the location and region for the identity.
- **Forwarding History** tab — displays the name of the person who forwarded the approval, the date the approval was forwarded and any comments. Approvals that are forwarded to or from a workgroup display the name of the workgroup. If there are multiple forwards, all ownership changes are displayed.

View Approval Line Item Details

Click the **Info** button for an individual approval item to see these Details.

For **Roles**:

- **Details** — displays the requested action and the name of the role. For Entitlement and account requests, information about the account and application is displayed.
- **Account Details** — displays the specific role name, the account name and the application for roles requests.
- **Entitlements** — displays the associated applications, attributes, entitlement name, and how it was assigned.

> **Note:** **If the requestor includes an Assignment Note when an approval request for a role and an account selection is required, the Assignment Note is displayed at the bottom of the Details tab.**

For **Entitlements**:

- A single panel listing the **Action**, **Attribute**, **Value**, **Account Name**, **Application**, and **Entitlement Owner**.

Track Request Details

To view detailed information about the requested items and any pending actions that still need to be taken on that request, click the Track Request Details option under the Actions (three-line) menu. This option is not available for some types of approvals, such as batch requests and native changes.

View Attachments

The attachments icon, paper clip, indicates if there are attachments included with this requested item and their number. Click the icon to display the attachment overlay containing the attachment list. Download to view the attachments from the list.

View and Post Comments

You can view or post comments for an approval, or for an individual approval item using the **Comments** button. The number next to the **Comments** button indicates the number of comments that exist for the approval or approval item. If no number is displayed, there are no current comments.

> **Note:** **For small form factors such a mobile phones, the Comments button is displayed in the Actions menu.**

You can perform the following tasks:

- "View Approval or Approval Line Item Comments" on page 293
- "Post Approval or Approval Line Item Comments" on page 294

View Approval or Approval Line Item Comments

Click the **Comments** button for the approval or approval item to view the comments. The Comments dialog lists the comments from the oldest to the newest with the oldest comments at the top. For each comment, the following information is displayed:

> **Note:** **All approvers can view all comments made by other users.**

- Posted comment
- Name of the user who posted the comment
- Date and time the comment was posted

Post Approval or Approval Line Item Comments

To post a new comment:

1. Click the **Comments** button for the approval or approval item

2. Type your comment in the text box at the bottom on the Comments dialog.

3. Click **Post**.

Chapter 35: Batch Requests

Batch Requests enable you to generate specific types of access requests for more than one user at a time. The required data is gathered from a prepared comma-delimited file for each request type. The batch files require comma-delimited data that represents the individual requests. In most cases the native identity or identity name can be used to specify the request target.

To access the Batch Request option, navigate to **Setup -> Batch Requests**.

> **Note:** **An identity must have IdentityIQ administrative capabilities to use this option. For information about setting up administrative capabilities, contact your IdentityIQ administrator.**

For more information, see:
- "Batch Request Types and Examples" on page 295 — provides descriptions and examples of the types of batch requests
- "Batch Requests Page" on page 299 — provides information on how to view, create, stop, or delete batch requests
- "Batch Request Details Page" on page 300 — provides information on how to view specific information about a batch request
- "Create Batch Request Page" on page 301 — provides information on how to import prepared comma-delimited files and set the parameters of the batch request.

Batch Request Types and Examples

This section describes the batch request types and criteria required in the comma-delimited file with examples. IdentityIQ supports the following types of batch requests:
- "Create Identity" on page 296
- "Modify Identity" on page 296
- "Create Account" on page 296
- "Delete Account" on page 296
- "Enable/Disable Account" on page 297
- "Unlock Account" on page 297
- "Add Role" on page 297
- "Remove Role" on page 298
- "Add Entitlement" on page 298
- "Remove Entitlement" on page 298
- "Change Password" on page 299

Batch request types with similar data and columns can be mixed in the same file. The following batch request types must be in a separate file:
- Create Identity
- Modify Identity
- Change Password

> **Note:** **To specify multiple entitlements or roles in the same request, use the pipe (|) delimiter to separate each role or entitlement.**

Create Identity

Use a Create Identity batch request to create a list of identities from a prepared comma-delimited spreadsheet. The operation in the spreadsheet for a Create Identity batch request is **CreateIdentity**.

Example:

operation, name, location, email, department
CreateIdentity, Alex Smith, Austin, asmith@adept.com, Accounting
CreateIdentity, Bob Smith, Austin, asmith@adept.com, Engineering
CreateIdentity, Mark Smith, Austin, asmith@adept.com, Accounting
CreateIdentity, John Smith, Austin, johnsmith@adept.com, Finance

-

Modify Identity

Use a Modify Identity batch request to modify or change the data of a list of identities from a prepared comma-delimited spreadsheet. The operation in the spreadsheet for a Modify Identity batch request is **ModifyIdentity**.

Example:

operation, identityName, location, email, department
ModifyIdentity, Alex Smith, Austin, asmith@adept.com, Accounting
ModifyIdentity, Bob Smith, Austin, asmith@adept.com, Engineering
ModifyIdentity, Mark Smith, Austin, asmith@adept.com, Accounting
ModifyIdentity, John Smith, Austin, johnsmith@adept.com, Finance

-

Create Account

Use a Create Account batch request to create accounts for a list of identities from a prepared comma-delimited spreadsheet. The operation in the spreadsheet for a Create Account batch request is **CreateAccount**.

Example:

operation, application, nativeIdentity | identityName, email
CreateAccount, AdminsApp, atoby, atoby@example.com
CreateAccount, AdminsApp, jsmith, jsmith@example.com

-

Delete Account

Use a Delete Account batch request to delete accounts for a list of identities from a prepared comma-delimited spreadsheet. The operation in the spreadsheet for a Delete Account batch request is **DeleteAccount**.

Example:

operation, application, nativeIdentity | identityName, email
DeleteAccount, AdminsApp, atoby, atoby@example.com
DeleteAccount, AdminsApp, jsmith, jsmith@example.com

-

Enable/Disable Account

Use an Enable/Disable Account batch request to enable or disable accounts on a specific application for a list of identities from a prepared comma-delimited spreadsheet. The operation in the spreadsheet for an Enable Account batch request is **EnableAccount**. The operation in the spreadsheet for an Disable Account batch request is **DisableAccount**.

Example:

operation, application, nativeIdentity | identityName
EnableAccount, AdminsApp, abell
EnableAccount, AdminsApp, jsmith
EnableAccount, AdminsApp, mjohnson

-

Unlock Account

Use an Unlock Account batch request to unlock application accounts for a list of identities from a prepared comma-delimited spreadsheet. The operation in the spreadsheet for an Unlock Account batch request is **UnlockAccount**.

Example:

operation, application, nativeIdentity | identityName
UnlockAccount, AdminsApp, abell
UnlockAccount, AdminsApp, jsmith
UnlockAccount, AdminsApp, mjohnson

-

Add Role

Use an Add Role batch request to add one or more roles to a list of identities from a prepared comma-delimited spreadsheet. The operation in the spreadsheet for an Add Role batch request is **AddRole**.

Example:

operation, roles, identityName
AddRole, Helpdesk Associate
AddRole, Benefits Manager, 222

AddRole, Accounting, 222
AddRole, Helpdesk Associate, 222

-

Remove Role

Use a Remove Role batch request to remove one or more roles from a list of identities from a prepared comma-delimited spreadsheet. The operation in the spreadsheet for a Remove Role batch request is **RemoveRole**.

Example:

operation, roles, identityName
RemoveRole, Helpdesk Associate, 122
RemoveRole, Helpdesk Associate, 132
RemoveRole, Helpdesk Associate, 143
RemoveRole, Helpdesk Associate, 156

-

Add Entitlement

Use an Add Entitlement batch request to add one or more entitlements to a list of identities from a prepared comma-delimited spreadsheet. The operation in the spreadsheet for an Add Entitlement batch request is **AddEntitlement**.

Example:

operation, application, attributeName, attributeValue, nativeIdentity | identityName
AddEntitlement, Procurement_System, group, @Audit, id1
AddEntitlement, Procurement_System, group, @Audit, id2
AddEntitlement, Procurement_System, group, @Audit, id3
AddEntitlement, Procurement_System, group, @Audit, id4
AddEntitlement, Procurement_System, group, @Audit, id5

-

Remove Entitlement

Use a Remove Entitlement batch request to remove one or more entitlements from a list of identities from a prepared comma-delimited spreadsheet. The operation in the spreadsheet for a Remove Entitlement batch request is **RemoveEntitlement**.

Example:

operation, application, attributeName, attributeValue, nativeIdentity | identityName
RemoveEntitlement, Procurement_System, group, @Audit, id1
RemoveEntitlement, Procurement_System, group, @Audit, id2
RemoveEntitlement, Procurement_System, group, @Audit, id3

RemoveEntitlement, Procurement_System, group, @Audit, id4
RemoveEntitlement, Procurement_System, @Audit, id5

-

Change Password

Use a Change Password batch request to change or reset passwords for a list of identities from a prepared comma-delimited spreadsheet. The operation in the spreadsheet for a Change Password batch request is **ChangePassword**.

Example:

operation, application, password, nativeIdentity | identityName
ChangePassword, Active_Directory, 1111, jsmith
ChangePassword, Active_Directory, 1111, mjohson
ChangePassword, Active_Directory, 1111, ajones

-

Batch Requests Page

Use the Batch Requests page to:
- View all batch requests that are assigned to you or to one of your workgroups
- View all batch requests that you requested
- Create a new batch request
- Stop or delete an existing batch request

You can perform the following tasks:
- View details about a batch request — Double-click on a batch request entry in the table. See "Batch Request Details Page" on page 300.
- Create a new batch request — Click New Batch Request at the top of the table. See "Create Batch Request Page" on page 301.
- Stop or delete a batch request — Right-click the batch request entry in the table.

View Batch Requests

To sort the information in the table by ascending or descending order, click the table header. Alternatively, mouse over the header row and use the drop-down arrow to select ascending or descending order. To select which rows are displayed:

1. Mouse over a header row.
2. Click the drop-down arrow.
3. Mouse over Columns to display the column options.
4. Use the check boxes to select which columns appear in the table.

Use the search field at the top of the table to filter the results of the Batch File Name column. Double-click a batch request line item to view the Batch Request Details page. Right-click a line item to Terminate or Delete the batch request.

Column Name	Description
Batch File Name	The file location where the batch file is originated.
Request Date	The date the batch request was generated.
Run Date	The date the batch request was executed.
Completed Date	The date the batch request was completed.
Record Count	The number of items within the batch request.
Status	The current status of the batch request. Scheduled — Batch request is scheduled to run at a later date. Running — Batch request is currently running. Executed — Batch request was run successfully. Terminated — Batch request process was cancelled.

•

Batch Request Details Page

Use the Batch Request Details page to view specific information about a batch request. The page is divided into two sections. The upper section provides information about the batch request as a whole including:

- File Name
- Date Requested
- Date Launched
- Date Completed
- Status
- Total Records
- Total Completed
- Total Errors
- Total Invalid

The lower section includes the Batch Request Items table which displays information for each record in the batch request.

Table 2—Batch Request Items Column Descriptions

Column Name	Description
Request Data	Displays the comma-delimited data of the requested operation.
Status	Displays the current status of the record's request. Running —Requested item is still processing. This could indicate an approval or manual work item completion is needed. Finished —The request process completed. Terminated — The request was manually cancelled. Invalid — Something was wrong with the request. Click the cell to show further details.
Result	Displays the result of the record's request. Success — The request completed. Failed — The request failed due to a general validation error. Approval —The request is waiting on an approval. ManualWorkItem — Indicates the request failed because the request type requires the generation of a manual work item and this was not a configured option in the batch request. PolicyViolation — The request failed because of a policy violation. ProvisioningForm —Indicates the request failed because the request type requires the generation of a provisioning form and this was not a configured option in the batch request. Skipped — Something was wrong with the request and it was skipped. Click the cell to show further details.
Identity Request ID	The request ID generated by the batch request. Note: You must select this option when you create the batch request.

-

Create Batch Request Page

Use the Create Batch Request page to import prepared comma-delimited files and set parameters of the batch request.

Table 3—Create Batch Request Configuration Options

Option Name	Description
Choose batch file	Click **Browse** and navigate the prepared comma-delimited file location.
Error handling	Determines the batch request process behavior in the event of an error. If a request item generates errors, you can continue the tasks or stop the task after a specified number of errors.
Policy Option	Determines the batch request process behavior for policy violations. You can include policy checking or to fail on any policy violation.

Table 3—Create Batch Request Configuration Options

Option Name	Description
Schedule to run	Choose to run the batch request immediately or select a later date and time when the request runs.
Manual input	Determines the batch request process behavior when a request needs manual interaction. You can skip batch requests which require additional manual input or create any necessary provisioning forms.
Work items	Determines the batch request process behavior when a request results in the generation of a work item. You can skip the request or create any necessary work items.
Handle create identity as modify if identity exists	Select this check box to handle a create identity batch request line item as modify identity request if identity exists.
Generate identity requests	Select this check box to create an identity request that can be viewed in Manage->Access Request.

•

Chapter 36: Lifecycle Events

Use the Lifecycle Events page to create new events or to configure existing events in your enterprise to trigger business process. When changes are detected during an identity refresh, IdentityIQ can be set up to launch event-based business processes.

> **Note:** **You must have IdentityIQ administrative capabilities to setup this function. For information about setting up administrative capabilities, contact your IdentityIQ administrator.**

To access Lifecycle Manager configuration pages, select **Lifecycle Manager** from the administrative setup menu.

For detailed setup information, refer to the IdentityIQ *Administration Guide*. The Administration Guide is located in your `IdentityIQ_InstallationDirectory\doc\pdf` directory, or click the link at the top of the online help Table of Contents to view a .pdf file.

Chapter 37: Lifecycle Manager Reports

Lifecyle Manager Reports enable you to monitor and analyze information about Lifecycle Manager requests.

The following reports provide information that is specific to the functions of Lifecycle Manager:

- "Access Request Status Report" on page 305
- "Account Requests Status Report" on page 306
- "Identity Requests Status Report" on page 307
- "Password Management Requests Report" on page 308
- "Registration Requests Status Report" on page 309

  Note: **An identity must have IdentityIQ administrative capabilities to use this option. For information about setting up administrative capabilities, contact your IdentityIQ administrator.**

- To access these report templates, navigate to **Intelligence -> Reports** and select a report from the list.
-

Lifecycle Manager Reports have the following sections:

- Standard Properties — see "Standard Report Properties" on page 193
- Parameters — see the individual report descriptions for their unique parameters.
- Report Layout — see "Report Layout" on page 194

  Note: **All reports use a set of standard properties to handle basic information, such as naming and descriptions, and controls settings. Controls include items such as scope and required sign off. You must enter the name before you run a report.**

The report information in the detailed results format can be exported to a .csv file and used in spreadsheets.

-

Access Request Status Report

The Access Request Status Report provides information associated with access request.

Use the following criteria to determine the information to use in this report. You can use any combination of options to build a report. You can use the Shift and Crtl keys to select multiple items from lists.

  Note: **If you select no options from a list, all options in the list are included in the report.**

Table 1—Access Request Status Report Entitlement Request Parameters

Option	Description
Applications	Type or use the drop-down list to select the applications to include in the report.
Approvers	Type or use the drop-down list to select the approvers to include in the report.

Table 1—Access Request Status Report Entitlement Request Parameters

Option	Description
Requesters	Type or use the drop-down list to select the requesters to include in the report.
Entitlements	Type or use the drop-down list to select the entitlements to include in the report.
Roles	Type or use the drop-down list to select the roles to include in the report.
Target Identities	Type or use the drop-down list to select the identities whose account is being modified to include in the report.
Status	Type or use the drop-down list to select **Completed**, **Approved**, **Rejected**, **Pending**, and **Cancelled**.
Requested Date Range	Specify a requested date range manually or click the calendar icon and select a date from the calendar
Finished Date Range	Specify a finished date range manually or click the calendar icon and select a date from the calendar

Account Requests Status Report

The Account Requests Status Report provides information associated with account requests.

Use the following criteria to determine the information to use in this report. You can use any combination of options to build a report. If you do not select options from a list, all options in the list are included in the report. You can use the Shift and Crtl keys to select multiple items from lists.

Table 2—Account Requests Status Report Account Request Parameters

Option	Description
Approvers	Select the approvers to include in the report. If no approvers are specified, all approvers are included. Click the arrow to the right of the suggestion field to display a list of all approvers, or enter a few letters in the field to display a list of approvers that start with those letters.
Requestors	Select the requestors to include in the report. If no requestors are specified, all requestors are included. Click the arrow to the right of the suggestion field to display a list of all requestors, or enter a few letters in the field to display a list of requestors that start with those letters.
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with those letters.
Target Identities	Select the target identity to include in the report. If no target identity are specified, all target identities are included. Click the arrow to the right of the suggestion field to display a list of all target identities, or enter a few letters in the field to display a list of target identities that start with those letters.

Table 2—Account Requests Status Report Account Request Parameters

Option	Description
Request Start and End Date(s)	The account request date range. The report provides all requests created on or after the start date and on or before the end date. You can enter the date manually, or click the **...** icon to select a date from the calendar.
Approval Start and End Date(s)	The account approval date range. The report provides all approvals created on or after the start date and on or before the end date. You can enter the date manually, or click the **...** icon to select a date from the calendar.
Status	Select the status to include in the report. If none are specified, all status levels are included.

Identity Requests Status Report

The Identity Requests Status Report provides information associated with identity requests including identity creation and editing.

Use the following criteria to determine what information to use in this report. You can use any combination of options to build a report. If you do not select any options from a list, all options in the list are included in the report. You can use the Shift and Crtl keys to select multiple items from lists.

Table 3—Identity Requests Status Report Identity Request Parameters

Option	Description
Approvers	Select the approvers to include in the report. If no approvers are specified, all approvers are included. Click the arrow to the right of the suggestion field to display a list of all approvers, or enter a few letters in the field to display a list of approvers that start with those letters.
Requestors	Select the requestors to include in the report. If no requestors are specified, all requestors are included. Click the arrow to the right of the suggestion field to display a list of all requestors, or enter a few letters in the field to display a list of requestors that start with those letters.
Target Identity	Select the target identity to include in the report. If no target identity are specified, all target identities are included. Click the arrow to the right of the suggestion field to display a list of all target identities, or enter a few letters in the field to display a list of target identities that start with those letters.
Status	Select the status to include in the report. If none are specified, all status levels are included.
Request Date Range	The identity creation request date range. The report provides all requests created on or after the start date and on or before the end date. You can enter the date manually, or click the calendar icon to select a date from the calendar.

Password Management Requests Report

The Password Management Requests Report provides information associated with password management actions.

Use the following criteria to determine what information is used in this report. You can use any combination of options to build a report.

Note: **If you do not select any options from a list, all options in the list are included in the report.**

Table 4—Password Management Requests Report Password Management Requests Parameters

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with those letters.
Requestors	Select the requestors to include in the report. If no requestors are specified, all requestors are included. Click the arrow to the right of the suggestion field to display a list of all requestors, or enter a few letters in the field to display a list of requestors that start with those letters.
Roles	Type or use the drop-down list to select the roles to include in the report. If no roles are specified, all roles are included.
Target Identity	Select the target identity to include in the report. If no target identity are specified, all target identities are included. Click the arrow to the right of the suggestion field to display a list of all target identities, or enter a few letters in the field to display a list of target identities that start with those letters.
Cause	Select the cause type to include in the report. If no cause types are specified, all types are included. Choose from the following types: **Expired Password** **Forgotten Password** **Change Request**
Status	Select the status to include in the report. If none are specified, all status levels are included.

Option	Description
Request Date Range	The edit identity request date range. The report provides all requests created on or after the start date and on or before the end date. You can enter the date manually, or click the **...** icon to select a date from the calendar.
Finished Date Range	The edit identity request completion date range. The report provides all requests that were completed on or after the start date and on or before the end date. You can enter the date manually, or click the **...** icon to select a date from the calendar.

Registration Requests Status Report

The Registration Requests Status Report provides information associated with registration requests. If you do not select any options from a list, all options in the list are included in the report.

The following criteria is used to determine what information is used in this report. You can use any combination of options to build a report.

Table 5—Registration Requests Status Report Identity Request Parameters

Option	Description
Approvers	Select the approvers to include in the report. If no approvers are specified, all approvers are included. Click the arrow to the right of the suggestion field to display a list of all approvers, or enter a few letters in the field to display a list of approvers that start with those letters.
Target Identities	Select the target identity to include in the report. If no target identity are specified, all target identities are included. Click the arrow to the right of the suggestion field to display a list of all target identities, or enter a few letters in the field to display a list of target identities that start with those letters.
Request Date Range	The edit identity request date range. The report provides all requests created on or after the start date and on or before the end date. You can enter the date manually, or click the **...** icon to select a date from the calendar.
Finished Date Range	The edit identity request completion date range. The report provides all requests that were completed on or after the start date and on or before the end date. You can enter the date manually, or click the **...** icon to select a date from the calendar.
Status	Select the status to include in the report. If none are specified, all status levels are included.

Registration Requests Status Report

Chapter 38: Lifecycle Manager Setup

Use Lifecycle Configuration to customize the availability and functionality of tools based on user needs. You can configure the following areas in Lifecycle Manager:

- Business Processes — sets the business process to use for specified Lifecycle Manager actions.
- Additional Options — sets additional customized options, such as full text searching, multiple role and account selection, and provisioning policies.

> **Note:** **An identity must have IdentityIQ administrative capabilities to use this option. For information about setting up administrative capabilities, contact your IdentityIQ administrator.**

To access Lifecycle Manager configuration pages, select **Lifecycle Manager** from the administrative setup menu.

For detailed setup information, refer to the IdentityIQ *Administration Guide*. The Administration Guide is located in your `IdentityIQ_InstallationDirectory\doc\pdf` directory, or click the link at the top of the online help Table of Contents to view a .pdf file.