SailPoint IdentityIQ

Version 8.1

Role and Group Management 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.

Chapter 1: Introduction to Roles, Workgroups, Populations, Groups

IdentityIQ offers several mechanisms for grouping Identities into sets based on shared characteristics. Each type of grouping has a distinct purpose and offers unique capabilities. This document explains the differences between them and the uses for each. They include:

- **Roles**: model the organizational structure, job functions, and system Entitlements. and present Entitlement data in a way that is readily understood by non-technical reviewers
- **Workgroups**: associate sets of Identities to facilitate sharing of IdentityIQ responsibilities; responsibilities can include Certification access reviews and Application or Entitlement ownership, among others
- **Populations**: query-generated lists of Identities that share a common set of attributes; used as a filter on the set of Identities included in a task, Certification, or report
- **Groups**: sets of Identities created based on the value of a single Identity Attribute; used as a filter on the set of Identities included in a task, Certification, or report.

Roles

IdentityIQ's Role functionality is used to model a company's structure and business operations. Roles are designed to be highly flexible and customizable, allowing them to be used to model a wide array of business structures and functions.

By default, there are four types of Roles configured in IdentityIQ:

- **Organizational**: organize and manage the role hierarchy
- **Business**: identify job functions or titles
- **IT**: encapsulate sets of system Entitlements
- **Entitlement**: represent individual system Entitlements

Custom Role types can be created to model a structure that doesn't easily fit into the IdentityIQ default model. In addition, the existing Role types can be configured to function differently from their default behavior to meet each organization's business needs.

A separate document has been created to explore all of these Role types. It offers some examples of how Roles can be used to model a business and to facilitate Identity management. Refer to the Role Management in IdentityIQ document for more information on Roles.

Workgroups

A Workgroup is a grouping of Identities that can be assigned activities within IdentityIQ as if the group were a single Identity. While a Role describes and manages activities and access outside of IdentityIQ, Workgroups specifically relate to activities and access within IdentityIQ.

Workgroups are primarily used in two ways: for allowing Identities to share responsibilities and for managing IdentityIQ Access for groups of Identities as a unit.

Responsibility Sharing

IdentityIQ allows activities or responsibilities to be assigned to Workgroups just as they can be assigned to an Identity. Grouping Identities into Workgroups makes it possible for multiple people to share responsibility for certain functions, which can help with managing activities that must be performed by someone but do not necessarily need to be owned or performed by a specific person.

The following activities are assignable to a workgroup:

- Application Owner
- Application Revoker
- Certification Owner
- Role Owner
- Entitlement Owner
- Account Group Owner
- Policy Owner
- Policy Violation Owner
- Policy Violation Observers

Consider, for example, a large-application System Administration team made up of 5 people who share responsibility for managing access and permissions for many users. These shared responsibilities could be divided among the team members by setting different team members as the Application Owner, Revoker, Certification Owner, etc. If, however, all team members are qualified and empowered to address any of these requests, it could be substantially more efficient to create a Workgroup for this team and assign these activities to the Workgroup, rather than assigning ownership to any one of the team members. Access/Revocation/Certification requests can then be funneled to the group to be processed by the first available team member.

IdentityIQ Access Management

System capabilities within IdentityIQ can also be managed for an entire population of Identities by assigning them to the same Workgroup. For example, if a help desk team all needs the same IdentityIQ capabilities, they can be assigned to a Workgroup and their access can be managed through the Workgroup instead of on each individual Identity. Capabilities set on individual Identities remain in effect in addition to the capabilities assigned to the Workgroup. If one person in the group, such as the team lead, requires additional IdentityIQ capabilities, the unique permissions for that person can be managed on their Identity without affecting the other group members' access.

Workgroup Creation

Workgroups are created on the **Setup** > **Groups** > **Workgroups** tab by clicking **Create Workgroup**.

A **Group Email** address can be specified, and emails can be configured to send to the group and/or the individual members. The group's common **Capabilities** and **Scopes** are specified in the **Rights** section, and Identities are added to the workgroup in the **Members** section at the bottom of the **Edit Workgroups** window.

About Populations and Groups

Populations and Groups are two more grouping constructs in IdentityIQ. Both of these are used subdivide identity sets within IdentityIQ for reporting and internal system tasks. Populations and Groups are created through different mechanisms, but they are used in similar ways throughout the IdentityIQ application.

Populations are sets of Identities generated from queries on the Advanced Analytics page and can be based on multiple criteria, such as North America, non-manager, accounting department employees. Any Identity Attribute marked as **Searchable** can be used as a Population criterion. The result set for the query (the Population) is a single set of Identities who share a common set of properties.

Groups are sets of Identities that share a common value for a specific Identity Attribute. Only Identity Attributes marked as **Group Factory** attributes can be used as a group filter attribute in the creation of Groups. Groups are usually created in sets. For example, generating groups based on the **Attribute Region** can produce a set of five groups: North America, Western Europe, Asia, South America, Eastern Europe.

When a Population or Group is saved, the query criteria to generate it is recorded and not the set of Identities that matched the criteria at that moment. Each time the Population or Group is used, the query is run and the current set of Identities matching the query criteria is retrieved and applied to the operation.

Creating Populations

To create Populations, you specify query criteria on the Advanced Analytics page of the IdentityIQ user interface (menu bar option and save it as a population. To access the Advanced Analytics page, from the Navigation menu bar go to **Intelligence -> Advanced Analytics**.

The UI provides two methods of specifying the criteria: the basic Identity Search and the Advanced Search windows. Identity Search allows you to specify simple filter values for Identity Attributes to define the population. With Advanced Search, you can be specify more complex search criteria, including grouping of filter criteria, choosing “and” vs. “or” relationships between criteria, and specifying search types other than “equals”.

Basic Identity Search

The default view of IdentityIQ's Advanced Analytics option is the Identity Search tab, which offers a variety of Identity Attribute for which search values can be entered. These criteria are evaluated together in an “and” relationship to select the population's members, meaning all Identities in the population will meet all search criteria specified.

In addition to basic Identity Attributes, application accounts held, detected or assigned Roles, associated Workgroups, and Risk Attributes can be used to filter Identities in a basic search.

Multi-Valued Attributes are specified separately, with the option of selecting multiple values in either “and” or “or” relationships (requiring the Identity to have all of the values assigned or any one of them, respectively).

The fields selected in the **Fields to Display** list are shown on the search results window. Once the search is saved as a population, however, the display fields do not really matter; when used in other parts of IdentityIQ as a processing filter, populations return the Identities that match the criteria, not just the specified display fields.

Once the parameters have been specified, click **Run Search** at the bottom of the window to execute the search based on the specified criteria.

To create the Population, click **Save Identities as Population** from the **Result Options** list.

Advanced Search

The Advanced Search options, accessible by clicking **Advanced Search** on the Identity Search tab, provide more flexibility in specifying search criteria.

Individual filters are specified by selecting a field, choosing a search type (such as equals, is greater than, is not equal to, is not null, et cetera) and entering a value (the Value field is suppressed for null/not null options). The "like" options can be further narrowed by whether the field value should start with, end with, contain anywhere, or be an exact match for the Value specified. Then, the filters can be connected through "and" or "or" relationships in any fashion, including grouping and nesting of criteria.

To edit the filter source directly, click [**view /edit filter source**]. This provides even more flexibility in specifying filter criteria in ways that might not be available through the user interface.

Once filters are modified through the filter source and saved, the standard representation of the search criteria is updated in the user interface to reflect the changes. When the variables selected are not ones the system is able to display in its reader-friendly format, the message **The filter you have entered cannot be displayed but will be applied to your search** is shown instead.

Filter Source Specification

Only persistent variables in the object model can be specified in the query filter. In general, this set matches the list of variables available through the public "get" and "set" methods shown in the IdentityIQ Javadocs that ship with the product. The variable names to specify match the method names without the "get"/"set" prefix. For example, the "**first name**" variable is accessible through the getFirstname() method, so the variable for the filter string would be firstname (the first letter of the variable name is always lowercase; the rest matches the camel case of the method name).

Fields within objects contained within the Identity object can be queried with the object.attribute syntax (for example, bundles.name or links.application.name). Multi-valued Identity Attributes can be accessed through the IdentityExternalAttribute object, and multi-valued Account Attributes can be queried through the LinkExternalAttribute object using syntax that mirrors the following:

```
IdentityExternalAttribute.collectionCondition("((id.join(IdentityExternalAttribute.
objectId) && IdentityExternalAttribute.attributeName i== \"IdentityAttributeName\"
&& IdentityExternalAttribute.value.startsWith(\"attributevalue\")))")
```

or

```
LinkExternalAttribute.collectionCondition("((links.id.join(LinkExternalAttribute.ob
jectId) && LinkExternalAttribute.attributeName i== \"AccountAttributeName\" &&
LinkExternalAttribute.value.startsWith(\"attributevalue\")))")
```

The table below indicates the syntax required to add filters of various data types to the filter source.

Table 1—Filter Syntax

Field Data Type	Structure	Example
String	"value"	department == "Accounting"
Numeric	value	location <= 10
Boolean	value	managerStatus == true
Date	DATE$[long value of time - milliseconds since Jan 1, 1970]	lastLogin > DATE$1318884600000

Table 1—Filter Syntax

Field Data Type	Structure	Example
Char (single character)	'value'	middleInitial == 'D'
Float	Value (floating point literal)	average < 250.144
Enumeration	EnumName.EnumValue	Type == CertificationItem.Type.Exception

Note: The IdentityIQ object model currently has no persistent Char or Float fields, and it is rare for Enumerations to be queried through these pages. Those three data types are included here primarily as interesting information.

The filter compiler can interpret the following operators and expressions:

Table 2—Operators and Expressions

Conditional Operators	&&, ||
Parentheses groupings and function references	(,), startsWith, startsWithIgnoreCase, endsWith, endsWithIgnoreCase, contains, containsIgnoreCase, in, inIgnoreCase, join, isNull, notNull, isEmpty, collectionCondition, subquery
Property Operators	==, !=, <=, >=, >, <, i==, i!=, i>=, i<=, i>, i< (i means ignore case)

Creating Groups

Three types of objects are involved in the creation of Groups:

- **Group Factory**: store the definition of which Attribute should be used for grouping and what to call the associated set of Groups
- **GroupDefinition**: contain the actual filter used to match identities to the group. Populations are also stored as GroupDefinition objects. Running the 'Refresh Groups' task scans the GroupFactories which in turn creates GroupsDefinitions for the values of the factory attribute.
- **GroupIndex**: also referred to as group scorecard; maintain statistics about a particular GroupDefiniiton (number of members, policy violations, composite risk score).

Groups are created on the Group Configuration window (menu option **Setup** > **Groups**) by clicking **Create New Group** on the Groups tab.

The **Name** field specifies what the GroupFactory will be called. A single **Group Attribute** is selected to define the selection criterion for membership in each of the created Groups; only Attributes that have been defined as "Group Factory" attributes can be used in creating Groups, so the selection list only includes those Attributes. When the Group is saved, a GroupDefinition is created for each value of that Attribute in the current set of Identities.

Identities' Group membership is determined at the time the Group is applied to an activity in IdentityIQ (such as when a Certification or a Task runs) based on the GroupDefinition filter. If an Identity's Group Attribute value changes, its new value is used for Group-based actions from the moment of the change. However, the statistics tracked in the GroupIndex, as well as the list of GroupDefinitions themselves, are only updated when an Identity Refresh task runs for which the **Refresh the group scorecards** option is selected. This means that if a new value is added for the Group Attribute (for example., in the Manager Group example above, a new manager is hired and assigned for a set of Identities), the new Group corresponding to that value will not be created or applied to any system activity based on the Group Factory until the refresh task runs.

Group and Population Definitions in XML

The XML representation of the Group Definition (filters defining a Population or Group) can be viewed and edited from the IdentityIQ debug pages by selecting **GroupDefinition**, clicking **List**, and then selecting the desired population or group name from the list.

The XML can be saved to create deployment artifacts that can be used for reimporting the definitions into a new environment. It can also allow one definition to be used as a template for creating others that can be imported into IdentityIQ instead of having to be generated through the user interface (for example, modifying the definition shown above, created for Location = Austin, to create an identical one for Location = Quebec).

Using Populations and Groups

Groups and Populations are used to apply actions in IdentityIQ to specific sets of Identities, rather than to every Identity in the system. They can be used in these areas:

- Filters on Identity Refresh and Policy Scan Tasks
- Advanced Certification selection criteria
- Advanced Analytics: Access Review and Activity Search query criteria
- Report Filters
- IT Role Mining Filters

Using Populations or Groups as filters for these activities makes it possible to run these queries and processes for select sets of Identities. By selecting only the desired Identities and omitting the rest from the process, these filters allow for targeted data analysis and more efficient system processing.

As Task Filters

Populations and Groups can be used as filters on Identity Refresh and Policy Scan tasks. These include all custom tasks created based on the Identity Refresh and Policy Scan task templates.

In Certifications

Advanced and Targeted Certifications can generate Access Reviews for specific Populations. Advanced Certifications can also generate Access Reviews for specific Groups. In Advanced Certifications, Population(s) or Group(s) are selected in the **What to Certify** section of the **Basic** page. In Targeted Certifications, Populations are selected in the **Who to Certify** section.

As Advanced Analytics Criteria

Two of the Advanced Analytics query types allow Populations to be used as search criteria: Access Review Search and Activity Search. The Access Review Search filter results in inclusion of only Access Reviews that were generated for the specified Population or Group. The Activity Search only allows Populations (not Groups) to be used as a filter limits the returned set of Identities to ones that are part of the selected Population.

As Report Filters

Populations and Groups can be used as filters on several of the pre-configured IdentityIQ reports, including the Advanced Access Review Report, the Identity Effective Access Report, the Identity Risk Report, and the Identity Role Report. The Advanced Access Review Report filter means the report is run only for Access Reviews created for the selected Population or Group. For the other reports, the filter allows only Identities that are part of the selected Population or Group to be included on the report.

In IT Role Mining

Populations can be specified as Identity selection criteria for IT Role Mining activities. Groups cannot be specified here.

Chapter 2: Role Management

This chapter contains the following sections:

- Role Modeling — used to create and maintain the roles that define your enterprise. See “Role Modeling” on page 11.
- Multiple Role and Account Assignment — roles can be assigned to the same identity multiple times, and roles can be applied to multiple accounts on the same application. See “Multiple Role and Account Assignment” on page 40.
- Automated Propagation of Role Changes to Role Members — any changes to the role or delete a role, that change would propagate to all identities that are currently assigned to the said role. See “Automated Propagation of Role Changes to Role Members” on page 43.

Role Modeling

Role modeling is used to create and maintain the roles that define your enterprise. These roles are used to categorize and manage users based on job function. Roles also provide a translation between business and IT functions, ease the provisioning and the request process for new access, simplify auditing, and the access review and certification process.

By default, there are four types of Roles configured in IdentityIQ:

- **Organizational**: organize and manage the role hierarchy
- **Business**: identify job functions or titles
- **IT**: encapsulate sets of system Entitlements
- **Entitlement**: represent individual system Entitlements

Roles are an important part of any 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 so that results and metrics can be understood and approved by business managers and executives.

Role mining enables you to create new roles within IdentityIQ by analyzing data within the system using pattern-matching algorithms. 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 within 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 within the enterprise. These roles typically model the IT privileges required to perform a specific function within 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 being monitored by IdentityIQ, the aggregation and correlation process discovers the entitlements, matches them to the roles you defined, and assigns those roles to the users who 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 within your business model. For example, type might be used to control inheritance or automatic assignment of roles. Role types are configured on the System Setup page.

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 within 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 impacted roles.

Granted IdentityIQ user rights enables you to associate specific IdentityIQ capabilities and scopes to roles. Those capabilities and scopes are then granted to identities when they are assigned the role and the Identity Cube Refresh task is run with the **Provision assigned roles option** selected. By default this function is disabled in IdentityIQ and must be turned on during the deployment and configuration process.

The Role Management page includes the following:

- "Role Search Tab" on page 21
- "Entitlement Analysis" on page 24
- "IT Role Mining" on page 26
- "Business Role Mining" on page 28
- "Working with the Role Manager" on page 33

Role Viewer Tab

Note: The Role Navigation panel can display roles that are outside of your assigned scope. You cannot edit those roles.

The Role Navigation panel of the Role Viewer tab displays your existing roles. The list of roles can be organized in a top down, bottom up, or grid format. The grid shows a simple list of roles in alphabetic order. If you expand a role in the Top Down view you see the roles that are members of the expanded role. If you expand a role in the Bottom Up view you see the roles in which the expanded role is a member. Use filtering to locate specific roles in the Top Down and Bottom Up views.

Click the arrow icon on the top, right side to contract or expand the Role Navigation panel. Contracting the panel provides more screen space to view role details in the Role Information panel.

Click a role to display detailed information in the Role Information panel of the Role Viewer.

If approval and impact analysis are active, roles and profiles that have changes pending approval or are undergoing impact analysis are displayed with a red square surrounding their icon. Role analysis and role approval

are an important part of the overall role life-cycle management. Role analytics and approval for new, modified, or rolled-back roles are controlled thought business processes configured for your implementation of IdentityIQ.

Inactive roles that are not pending approval or analysis are displayed with a gray icon.

To add a new role, click **Add** or **New Role > Role** to open the Role Editor page. Right-click an existing role and select **Clone** to create a new role based on the existing one. See “Role Editor Page” on page 15

To delete a role, right-click the role and select **Delete**, then confirm the deletion request.

The Role Information panel contains all of the information associated with the selected role. Some of the sections listed in the table below may not be available for all role types. If there is information associated with a role that is not supported by the assigned role type, the information is displayed with a warning message.

Roles in which activation rules are enabled display a notice in the upper right-hand corner of the information panel containing activation or deactivation information.

Table 3—Role Viewer - Information Panel Descriptions

Field Name	Field Description
Name	The name of the role.
Display Name	The name to be used throughout IdentityIQ.
Owner	The owner assigned to the role.
Scope	The scope of this role. Scope is used to determine the objects to which a user has access. If scoping is active, identities can only see objects that they created or that are within the scopes they control. **Note: The scope option is only displayed if the scope feature is enabled.**
Type	The type of role being displayed. Role type definitions are customizable and created as part of the configuration process.
Description	A short description of the role.
Extended Attributes	Any extended role attributes configured for your enterprise and marked as searchable are displayed with the role information. For example, Identity Attribute, Date Attribute, Rule Attribute.

Table 3—Role Viewer - Information Panel Descriptions

Field Name	Field Description
Role Statistics	The Role Statistics panel displays detailed statistical information on the users and entitlements a given role. Click each applicable category to view a window containing item-specific statistical information. Available IdentityIQ categories include the following: **Members** - Number of Identities assigned the role. Click to view a grid displaying those identities. **Members with Additional Entitlements** - Number of Identities that have entitlements which are not permitted or required by this role or any other role they have been assigned. This applies to Business Roles provided by IdentityIQ, not to custom roles. **Members with Missing Required Roles** - Number of Identities that are missing roles which are required by this one. This applies to Business Roles provided by IdentityIQ, not to custom roles. **Identities Detected** - Number of Identities whose entitlements indicate that they have this role. Click to view a grid displaying those identities. This applies to IT and Entitlement Roles provided by IdentityIQ, not to custom roles. **Identities Detected to be Exceptions** - Number of Identities whose entitlements indicate that they have this role, even though they have not been assigned any roles that permit or require this one. Click to view a grid displaying those identities. This applies to IT and Entitlement Roles provided by IdentityIQ, not to custom roles. **Provisioned Entitlements** - Number of Entitlements that would be provisioned if this role were to be assigned to and/or required by a new Identity. This applies to Business, IT, and Entitlement Roles provided by IdentityIQ, not to custom roles. **Permitted Entitlements** - Number of Entitlements that would be provisioned in order for an Identity to match all roles permitted by this one. This applies to Business Roles provided by IdentityIQ, not to custom roles. Click the **Refresh** button at the bottom of the panel of each role you wish to view the statistics. -OR- Run the **Refresh Role Scorecard** task to populate and display the statistical data by default on all roles. Note: The “Refresh role metadata” option must be selected in the Refresh Identity Cubes task in order for Role Statistics panel to display any information.
Scheduled Events	The events scheduled for this role. **Activate** — the date on which the role becomes active. **Deactivate** — the date on which the date is to be deactivated.
Archived roles	Previous, or different, versions of this role. If archiving is active, each time a change is made to a role definition a version of the role is stored. This enables you to roll-back to previous versions if required.

Table 3—Role Viewer - Information Panel Descriptions

Field Name	Field Description
Assignment Rule	The rule used to automatically assign roles to identities during a correlation process. Roles assigned either manually on the identities pages or through an assignment rule are considered Assigned Roles throughout IdentityIQ.
Inherited Roles	The roles in which this role is a member.
Permitted Roles	Roles to which users have access if they are assigned this role.
Required Roles	The roles to which the user must have access if they are to be assigned this role.
Entitlements	The rules and permissions (targets and rights) that define the profiles contained within the role. The entitlements are grouped by application.
Inherited Entitlements	The entitlement details for the entitlements that define the roles to which this role is a member. The included entitlements are grouped by application.
Granted IdentityIQ User Rights	The IdentityIQ capabilities and scopes associated with role. These rights are granted to the identities to whom this role is assigned. **Note: These capabilities and scopes are not assigned until a Identity Cube Refresh task is run with the Provision assigned roles option selected.**

The Role Viewer tab enables you to work with the following IdentityIQ components:

- Roles — See “Role Editor Page” on page 15
- Archived Roles — See "Role Editor - Archived Role Panel" on page 18
- Profiles — See "Role Editor - Edit Entitlement Panel" on page 18

Role Editor Page

Use the Role Editor to define the roles for your enterprise. A role is a collection of entitlements or profiles that enable an identity to perform certain operations. For example, one role might enable an identity to request a purchase order and another might enable an identity to approve purchase requests. Use roles to monitor identity entitlements, identify policy violations, and compile identity risk scores to enable you to maintain compliance.

Note: When adding new roles, the list of attributes changes to reflect the currently selected role type. When editing a role, if the role type changes, any attributes from the original role are preserved and the user is prompted with the warning message “This attribute does not apply to the current role type”.

Click **Submit** to save the changes made on this page. Click **Submit with Impact Analysis** to save the changes and create an impact analysis report. the report provides details on the impact these changes have on the rest of your product implementation and statistics on the amount of overlap between the new role and existing roles. If the approval business process is active, an approval work item is sent to the role owner and the role changes are inactive until the approval is complete. See “How to Approve Role Changes” on page 39 and "How to Perform Impact Analysis" on page 39.

Roles that are awaiting approval are displayed with a red square around the role icon. You can further edit roles with approval or analysis pending, but a notice displays at the top of the page alerting you that “An approval or impact analysis work item is pending on this role.” If you change and submit a role with changes pending, the original work item is deleted and replaced with a work item containing the latest changes. A role with changes pending approval displays the original, unchanged, role information on the Role Information panel, but the latest,

changed, information on the Role Editor page. This enables you to view the role as it currently exists in the Role Information panel, but ensures that you do not duplicate changes on the Role Edit page.

See “How to Create or Edit a Role From the Role Management Page” on page 33 for information on how to work with roles.

The Role Editor panel contains all of the information associated with the selected role. Some of the sections listed in the table might not be available for all role types. If there is information associated with a role that is not supported by the assigned role type, the information is displayed with a warning message.

Table 4—Role Management - Role Editor Field Descriptions

Field Name	Description
Name	The name of the role.
Display Name	The name to be used throughout IdentityIQ.
Type	The type of role. For example, organizational, business, or IT. Role type definitions are customizable and created as part of the configuration process.
Owner	Enter a valid user or workgroup. Typing the first few letters of a name displays a list of all of the user and workgroup names in the system containing that letter combination. You can select from the displayed list.
Scope	Select a scope from the drop-down list. Only scopes that you control are displayed in the list. Scope is used to determine the objects to which a user has access. If scoping is active, identities can only see objects that they created or that are within the scopes they control.
Description	A brief description of the role. **Note: This description is displayed with the role throughout IdentityIQ and should be as intuitive as possible.** 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 is the description used by default. **Note: You must Save the description before changing languages to enter another description.**
Classifications	Classifications are used to categorize and flag a role, to identify it as potentially allowing access to sensitive, privileged, or otherwise significant data.
Enable Activity Monitoring	Activate this feature to track activity for any user who is assigned this role. If activity monitoring is not available on the selected application, the Activity Monitoring Enabled check-box is replaced by the following note: This application does not currently have activity monitoring configured.
Provision both profiles and policies	Provision any changes to either profiles or policies associated with this role.

Table 4—Role Management - Role Editor Field Descriptions

Field Name	Description
Allow multiple application accounts	Enables a role to specify its own target account, or create a new account, during a role request, even if it is required by another role and included in that roles required roles list. If this option is not enabled, required roles are assigned to the same account as the top-level role.
Enable multiple assignments	**Note: This option is not available if either multiple assignments are not enabled, or if they are universally enabled.** Enables a role to be assigned to the same identity multiple times. This option is only available on assignable role types.
Disable	Disable the role so that it is no longer available in your application. Disabled roles names appear gray in the Role Navigation panel.
Custom or Extended Role Attributes	Any extended role attributes configured for your enterprise and marked as searchable are displayed with the role information.
Scheduled Events	The activation events scheduled for the role. Activation events use business processes to automatically activate or deactivate roles based on the dates specified in the Add New Event dialog.
Assignment Rule	A rule used to automatically assign roles to identities during a correlation process. Assignment rules can be created using: **Match List** — only identities whose criteria match that specified in the list. The criteria is configured using the tools provided. Add identity attributes, application attributes and application permissions. Customize further by creating attribute groups to which this assignment rule applies. Note: If Is Null is selected, the associated value text box is disabled. When the is null match is processed, the term matches users on the chosen application who have a null value for that attribute/permission. **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 and assign this role to identities in that population.
Permitted Roles	Roles to which users have access if they are assigned this role.
Required Roles	The roles to which an identity must have access before this role can operate properly.
Inherited Roles	The roles in which this role is a member.
Entitlements	Detailed information about the entitlements that are contained in the role. Use this panel to create new entitlements or edit or delete existing entitlements. Mouse over the information icon to display the description of an entitlement.

Table 4—Role Management - Role Editor Field Descriptions

Field Name	Description
Provisioning Policy	A list of provisioning policies associated with this role. Use this panel to add, edit, or delete provisioning policies.
Granted IdentityIQ User Rights	Use this panel to specify the IdentityIQ capabilities and scopes associated with role. These rights are granted to the identities to whom this role is assigned. **Note: These capabilities and scopes are not assigned until a Identity Cube Refresh task is run with the Provision assigned roles option selected.**

Role Editor - Archived Role Panel

Click an archived role to display the Archived Role panel and view the details of the archived role and determine the proper version for this roll-back.

Click **Roll Back to Archive Role** to return to the Role Editor page. Use the action buttons on the bottom of the page to complete the procedure. If approval is required on role changes it is required when a role is rolled back to a previous version.

Role Editor - Edit Entitlement Panel

Use the Edit Entitlement panel to define the profiles that are included in the role. A profile is a set of entitlements on an application. An entitlement is either a specific value for an account attribute, most commonly group membership, or a permission. Profiles are not shared between roles.

Click **Submit** to save changes or add the profile to the role.

Note: The simple view might not be available for all roles.

There are two options for adding entitlements to a role, the **Simple View** or the **Advanced View**. The simple view eliminates the need to create attribute rules to locate entitlements and provides a drop-down list of the entitlement configured for selection for each application. See “How to Create or Edit a Profile” on page 35 for information on how to work with profiles.

The Entitlement Editor panel contains the following information:

Table 5—Role Editor - Edit Entitlement Panel Simple View Field Descriptions

Field Name	Description
Application	The application associated with the account attributes or permissions for this profile.
Account Attribute	The value of the account attribute, most commonly group membership.
Select Entitlement	Specify as many entitlements as required for this role.

Table 6—Role Editor - Edit Entitlement Panel Advanced View Field Descriptions

Field Name	Description
Description	A brief description of the profile. **Note: This description is displayed with the role throughout the product and should be as intuitive as possible.**

Table 6—Role Editor - Edit Entitlement Panel Advanced View Field Descriptions

Field Name	Description
Application	The application associated with the account attributes or permissions for this profile.
Attribute Rules: Attribute rules are made up of filters that can be grouped and controlled using AND\OR operations. The attribute rules associated with a profile can be as simple or complex as needed. The Add a Filter box is used to create the individual filters, the Filter(s) box is used to view and manipulate the existing filters. See "How to Create or Edit a Profile" on page 35.	
Field	The attribute associated with the attribute filter. The drop-down list contains all attributes configured for the selected application. Applications are configured on the Configure Application page.
Search Type	The qualifier associated with the attribute value. **Multi Valued attributes** — contains all, is null, is not null **Long, Int, Date** — All except contains all and is like — equals, is less than, is greater than, is greater than or equal to, is less than or equal to, is in, is null, is not null, is not equal **Boolean** — equal, is not equal to, is null, is not null **Permission** — equals, is not equal, is in, is null, is not null **Everything else** — All operations except contains all — is like, equals, is less than, is greater than, is greater than or equal to, is less than or equal to, is in, is null, is not null, is not equal
Value	**Note: This field is not available for unary operations.** The value of the attribute. When available, select an entitlement from the drop-down list.
Ignore Case	Specifies if case should be a factor when comparing entitlements defined for profiles with those assigned to users. During identity correlation, the entitlements defined in profiles are compared with entitlements assigned to users to determine roles and additional entitlements for certifications. This field is not available for unary operations.
Operation	The operation used to control the interaction between the filters.
Permissions:	
Rights	The rights associated with this profile on the target attribute. For example, create, read, update, delete, execute. Use the Shift and Ctrl keys to select multiple rights from the list.
Target	The target attribute for this permission.

Role Editor - Provisioning Policy Editor Panel

Provisioning policies define the fields required for a role to be provisioned, often including a default value or script/rule for calculating a value. With a provisioning policy in place, when a role is requested and a field cannot be calculated by the system, the user must input specified criteria into a generated form before the request can be completed.

See "How to Create or Edit a Provisioning Policy" on page 21 for information on how to work with provisioning policies.

The Provisioning Policy Editor panel contains the following information:

Table 7—Role Editor - Provisioning Policy Editor Field Descriptions

Field Name	Description
Edit Provisioning Policy Fields Panel Use the Edit Provisioning Policy Fields panel to customize the look and function of the form fields generated from the provisioning policy.	
Name	The name of the field.
Display Name	The name displayed for the field in the form generated by the provisioning policy.
Help Text	The text you wish to appear when hovering the mouse over the help icon.
Type	Select the type of field from the drop-down list. Choose from the following: Boolean — true or false values field Date — calendar date field Integer — only numerical values field Long — similar to integer but is used for large numerical values Identity — specific identity in IdentityIQ field Secret — hidden text field String — text field
Multi Valued	Choose this to have more than one selectable value in this field of the generated form. Click the plus sign to add another value.
Read Only	Determine how the read only value is derived: Value — value based on the selection from the drop-down list Rule — value is based on a specified rule Script — value is determined by the execution of a script
Hidden	Determine how the hidden value is derived: Value — value based on the selection from the drop-down list Rule — value is based on a specified rule Script — value is determined by the execution of a script
Owner	The owner of the provisioning policy. This is determined by selecting from the following: None — no owner is assigned to this provisioning policy. Application Owner — identity assigned as owner of the application in which the provisioning policy resides. Role Owner — identity assigned as owner of the role in which the provisioning policy resides. Rule — use a rule to determine the owner of this provisioning policy. Script — use a script to determine the owner of this provisioning policy
Required	Choose whether or not to have the completion of this field a requirement for submitting the form.
Review Required	Choose whether or not to require the person who is approving the workflow item to approve this field.
Refresh Form on Change	Select this option to have the form associated with this policy refresh to reflex changes to this policy.

Table 7—Role Editor - Provisioning Policy Editor Field Descriptions

Field Name	Description
Display Only	Set this field as display only.
Authoritative	Boolean that specifies whether the field value should completely replace the current value rather than be merged with it; applicable only for multi-valued attributes
Value	Determine how the value is derived. Select from the following: Literal — value is based on the information you provide Rule — value is based on a specified rule Script — value is determined by the execution of a script
Value	The value displayed in the field of the generated form before editing. Choose from the following: None — the field is blank Literal — value is based on the information you provide Rule — value is based on a specified rule Script — value is determined by the execution of a script
Validation	Gives the ability to specify a script or rule for validating the user's value. For example, a script that validates that a password is 8 characters or longer.

How to Create or Edit a Provisioning Policy

To Create or Edit a Provisioning Policy:

1. Access the Provisioning Policy panel from the Role Editor page.
2. Click an existing provisioning policy to edit or click Add Provisioning Policy to create a new one.
3. Edit the provisioning policy information.
4. Optional: Add or delete provisioning policy fields.
   See "Role Management - Role Editor Field Descriptions" on page 16 for descriptions of the fields in each section.
5. Select fields to include in the form.
6. Click **Save** to return to the Role Editor.

Role Search Tab

Use the Role Search tab to generate searches on the roles. These searches can be used to locate roles by name, owner, type, or status. You can also search for roles by the number of users to whom they are assigned, either 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 can yield results.

Searches yielding helpful results can be saved for your reuse, or saved as reports. Saving a search as a report enables scheduling of the search on an on-going basis for monitoring and tracking purposes.

The search fields are inclusive, only actions matching values specified in all fields are returned with the results.

Search criteria is used to narrow the result set for a search. Not entering information or making a selection in a search criteria field implies that all possible choices should be included. For example, if you do not enter an type in the **Type** field, events with any action type are included.

The Role Search tab contains the following information:

Table 8—Role Management - Role Search Criteria

Criteria	Description
Saved Searches:	
Search Name	The names of past searches that you have saved for reuse. **Note: These Saved Searches are only available for your use.**
Loaded Saved Search:	
The name and description of the saved query with which you are working.	
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.
Role Attributes:	
Name	Enter a role name on which to 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 returns information for the roles System Administrator, SysAdmin, and Administrative Assistant.
Owner	Enter the role owner on which to 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 whose names start with that letter string.
Type	Select the role type on which to search. For example, IT, Organizational, or Business. Role types are defined for your enterprise during the role modeling process.
Status	Select the status of the roles to include in the search, Enabled or Disabled.
Classification	Select a classification to include in the search.

Table 8—Role Management - Role Search Criteria

Criteria	Description
Detected Total	Specify an upper or lower limit to the number of identities by whom this role can be detected and still 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. This search returns 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 to whom this role can be assigned and still be included in the search results. Assigned roles are roles that were manually assigned to an identity by someone 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. This search returns all roles that were not manually assigned to at least one identity.
Entitlement Total	Specify an upper or low limit to the number of entitlements a role can contain and still be included in the search results. For example, if you select Less Than and type `3`, the search returns roles that contain two (2), one (1), or zero (0) entitlements.
Risk Score Weight	Specify an upper or lower limit for risk score weight that can be 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 only roles that are associated with at least one other role or only roles that are not associated with any other role. **True** — include only roles that are associated with at least one other role. **False** — include only roles that are not associated with any other roles.
Filter By: Date	

Table 8—Role Management - Role Search Criteria

Criteria	Description
Date Type	Select a state with which to relate the dates specified: Last Membership Certification — the date the last role membership certification was performed. Last Composition Certification — the date the last role composition certification was performed. Last Assigned — the date the role was last assigned to an identity.
Start Date	Specify a beginning date for this search. The search returns information pertaining to any action performed on or after the date specified.
End Date	Specify an end date for this search. The search returns information pertaining to any action performed on or before the date specified.
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. **Note: You must select at least one field to display on the results page.**

Role Search Results

The Role Search Results panel displays all of the roles that match the criteria specified in your search. The results are dependent on the **Fields to Display** list on the Role Search tab. From the Role Search Results panel you can export your search results to file and save the search criteria for use in the future.

Searches Options:

Use the drop-down list above the Role Search Results panel to save search criteria for use in future searches:

- **Save Search** — save the search for your own use. A list of saved searches is displayed at the top of the search tab each time you log in.
- **Save Search as Report** — searches saved as reports are added to your list of reports and can be scheduled to run on an on-going basis See “Reporting” on page 407.

Export Searches:

Use the buttons on the top, right of the Role Search Results dialog to export the search results to file for archiving and auditing purposes. The search results can be exported to an Adobe PDF or Microsoft Excel format.

Entitlement Analysis

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

Entitlement analysis enables you to search for entitlements based on specific application and identity information or by populations defined within your deployment of IdentityIQ. This feature enables you to create meaningful roles without having to remember every entitlement on every application or be familiar with the access assigned to each employee in your enterprise.

Entitlement Analysis also enables you to analyze the entitlement information collected to further refine the roles you are creating before saving.

Performing Entitlement Analysis involves three distinct phases:

- Searching for entitlements
- Analyze the search results
- Creating roles

Search for Entitlements:

1. Access the Entitlement Analysis tab from the Role Management page.
2. Select the applications on which to search for entitlements.
   Enter the first letters of an application name to display a suggestion list, or click the arrow to the right of the field to display a list of all the applications to which you have access.
3. *Optional:* Narrow your entitlement search using the Identity Attribute fields or a list of populations.
   Use the **Search by Attribute** or **Search by Populations** radio buttons to switch between the options.
   The Identity Attribute fields displayed are dependent on the identity attributes defined during configuration. Populations are defined from the Advanced Analytics, Identity Search Results page.
4. Click **Search** to begin the entitlement mining based on the specified criteria.

Analyze the Search Results:

The search returns the following information:

Note: The search only returns those entitlements based on account or group attributes, not those based on permissions.

Table 9—Role Management IT - Role Analysis Search Results Descriptions

Column	Description
Search Parameters:	
Attribute	The criteria used to define this search. For example, Application, Last Name, Population, or Manager.
Filter Type	The type of filter applied to the search criteria. For example, Equal or Like.
Value	The value entered in the search field.
Only show percentages above: Use the slider to limit the results displayed in the table based on the percentage of the population to which the results apply. For example, if you are only interested in entitlements that apply to at least forty percent (40%) of the population searched, click the slider and move it to that percentage, or type the percentage in the field to the right.	
Entitlement Information: Click a value to display a list of all identities to whom that entitlement is assigned.	
Name	The name of the attribute from which this entitlement was derived. Attributes used to define entitlements are specified during configuration.
Value	The value assigned to the attribute. Click a value to expand a list of users to whom the entitlement is assigned.
Percent of Population	The number of identities assigned to that value of that attribute on this application expressed as a percentage of all identities that have an account on the application.

Use the results to analyze the entitlements that exist within your enterprise. The Group and Analyze feature enables you to group entitlements within an application and generate results based on that group. This feature enables you to see how assigning multiple entitlements to a role can impact access within the application.

To group and analyze, select multiple entitlements and click **Group and Analyze**. The results are displayed below the entitlements table. Click a group to see the details for the entitlements within. You can perform analysis multiple times on entitlements or on the groups created.

Save the Profile:

When you are satisfied with the information you have mined and analyzed, click **Create Role**. You must enter an name for the new role, optionally a type and description, and click **Save** to return to the Role Viewer.

Additional Information

From the Role Editor you can add additional profiles, edit the role or save the role and return to the Role Viewer. See “Role Editor Page” on page 15.

Role Mining

Role Mining is used to create roles based on specified criteria in an existing enterprise. IdentityIQ separates role mining into the following categories:

- "IT Role Mining" on page 26
- "Business Role Mining" on page 28

The IT Role Mining panel generates roles in bulk. The population of identities from which to mine can be restricted by IPOP or by String, boolean, or integer attributes (multi-valued are not supported at this time).

The entitlements from which roles are generated are defined on a by-application basis. When an application is added to the mining analysis, all of its entitlements are added to a box to the right. Users can prevent the entitlements from being considered in the analysis by clicking the “x” next to them.

The population size is restricted by the defined identity population as well as the applications under consideration. The current population size is presented along with a warning that mining details are not available for large populations.

You can restrict the roles that are generated by specifying a minimum number of identities and entitlements per role.

Select IT Role Mining or Business Role Mining from the Create New drop-down list to create and launch a new role mining task. Alternatively, you can select an existing template from the Role Mining Template panel and use the predefined criteria in your role mining task.

Note: Names are required when creating role mining templates. When you edit an existing template, you are given the choice to either change the existing template or create a new template. If you create a new template you are require to give it a new name.

IT Role Mining

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

The mining task generates or updates a single IT role with entitlements that are mined from a user population specified by groups, applications, or an identity filter. A threshold percentage limits the entitlements that are added to those held by a percentage of the population that exceeds the threshold.

Create New IT Role Using Role Mining

Use the Create New drop-down list at the top-right corner of the page and select IT Role Mining. Input your mining criteria in the IT Role Mining panel. View "Role Management - IT Role Mining Field Descriptions" on page 27 for details about the IT Role Mining panel.

Table 10—Role Management - IT Role Mining Field Descriptions

Field Name	Description
Owner	Enter a valid user or workgroup. Typing the first few letters of a name displays a list of all of the user and workgroup names in the system containing that letter combination. You can select from the displayed list.
Identities to Mine	Search By Attributes – Input the attribute data to target specific identity criteria used in the role mining task. Search By Population – Select a population on which the role mining task is run. Note: Selecting a population automatically filters the applications to those included in the selected population.
Applications to Mine	Specify the application(s) on which to focus the mining task.
Entitlements to Exclude	Select any entitlements that are associated with the application to exclude in the role mining task. All other entitlements are used as part of the role mining criteria.
The size of the population to be mined is currently X identities	The variable value of the total number of identities used in the role mining task based on the current mining criteria.
Minimum Identities per Role	Specify the minimum number of Identities, who meet the role mining criteria, that are required to create this role.
Minimum Entitlements per Role	Specify the minimum number of entitlements, which meet the role mining criteria, that are required to create this role.
Maximum Groups to Mine	Specify the maximum number of groups (candidate roles), which can be generated using this role mining criteria. Note: The role mining task fails if the number of candidate roles discovered exceeds the number specified in this field.

Once you have entered your criteria, click **Save** to save your selections as an IT Role Mining template. Click **Save and Execute** to save the template and run the role mining task. Enter the name of your role mining template then click OK.

Use An Existing IT Role Mining Template

Use or edit an existing IT Role Mining template to generate a role based on previous criteria by clicking a template name in the Role Mining Templates panel on the Role Mining tab.

Click **View Latest Mining Results to view the results of the most recent mining task for this template**.

Any changes to the template are saved for this template unless the template name is changed. Once you have entered your criteria, click **Save** to save your selections, or click **Save and Execute** to save the template and run the role mining task. Executed mining tasks appear on the Role Mining Results tab.

Note: Names are required when creating role mining templates. When you edit an existing template, you are given the choice to either change the existing template or create a new template. If you create a new template you are require to give it a new name.

Business Role Mining

Business role mining within 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. The criteria used to generate the business role can be saved as a template for future use. After the mining task is completed, the new roles are added to the Role Viewer where they can be modified as necessary.

The Business Role Mining panel generates roles from identity attributes and entitlements. The generated roles are either organized into a hierarchy based on identity attributes of the users from which the roles are mined or they are generated in a flattened manner. From there they are moved into either an existing container role or one that was newly created.

Entitlement mining is optionally performed on the generated business roles. These entitlements are either directly attached to those business roles or place in newly created IT roles that are then added to the business roles' Permits or Requires lists.

Once you have entered your criteria, click **Save** to save your selections as a Business Role Mining template, or click **Save and Execute** to save the template and run the role mining task. Enter the name of your role mining template then click **OK**. When the task is launched a success message dialog is displayed.

If you perform role mining on the same role consecutive times, the process does not modify owner, assigned scope, description, type, selector, or the disabled attributes on consecutive runs. Sub roles can be added on consecutive runs, but not removed. Mining for entitlements does not change. The process mines and associates entitlements. If a role is enabled and mining is run again, the role remains enabled, and entitlements can be granted with no approval process. If a role is disabled before the repeated mining is run, the role remains disabled.

To review the results of the mining task, click **View Latest Mining Results**. See “Role Mining Results” on page 31.

The roles generated by the mining task are displayed on the Role Viewer tab.

Once the roles are created and active they can be used just like any other roles.

Note: Roles created through business role mining are disabled by default.

To clear the role mining form, click **Reset Mining Form**.

Table 11—Role Management - Business Role Mining Field Descriptions

Field Name	Description
General Settings:	
Name	The name of the business role mining routine. The name created here is used to identify the settings used in the event the same role mining routine is reused in the future.

Table 11—Role Management - Business Role Mining Field Descriptions

Field Name	Description
Compute Population Statistics	Compute statistics for the mined roles and display them in the task result.
Perform Analysis Only (no roles are generated)	Perform the role mining for analysis purpose only. No roles are generated when this mining is complete. See the results of the task on the Task Results tab of the Tasks page.
Hierarchical Settings:	
Generate a New Root Container Role	Generate a container role into which all generated roles should be placed.
Specify an Existing Root Container Role	Select an existing role into which all the newly generated roles should be place.
Generate a Role Hierarchy from the Identity Mining Attributes	Generate a role hierarchy. Each attribute generates its own level in the hierarchy, and that level contains the roles whose names match the values for that given attribute.
Ordered Identity Mining Attributes	Arrange the list of attributes used to order the hierarchy of the generated roles. Users are assigned the role based on this list's ordering. For example if the list order is 1. Region, 2. Location, 3. Department then all users in the same department for a given location in a given region are assigned that role.
Role Settings:	
Type of Business Roles to Generate	Type of role generated by the task. Note: This option is hidden when the “Perform Analysis Only” is selected on the business role mining page.
Owner	Enter a valid user. Typing the first few letters of a name displays a list of all of the user names in the system containing that letter combination. You can select from the displayed list. Note: This option is hidden when the “Perform Analysis Only” is selected on the business role mining page.
Minimum Number of Users per Role	Minimum number of users who must the mining criteria before a role is generated.
Naming Algorithm	The filter-based naming algorithm concatenates all the attributes, separated by periods, to generate role names. The generic UID naming algorithm generates random role names. Note: This option is hidden when the “Perform Analysis Only” is selected on the business role mining page.

Table 11—Role Management - Business Role Mining Field Descriptions

Field Name	Description
Prefix to Apply to Generated Role Names	Prefix to add to the generated role names. Note: This option is hidden when the “Perform Analysis Only” is selected on the business role mining page.
Disable Generated Roles	Disable all newly generated roles upon creation. This enables you to review and modify the roles if necessary before they are available for use.
IT Settings:	
Mine for Entitlements on Generated Business Roles	Mine for entitlements as part of this task.
Attach Mined Profiles directly to Business Functional Roles	Attach mined profiles directly to the generated roles. If this option is not selected new IT roles are created to hold the entitlements and these IT roles are added to the generated roles' Permits or Requires list based on the selection below.
Type of IT Roles to Generate	Type of role that is generated to hold the entitlements.
Business Roles' Relationship to Mined IT Roles	Determines if the newly created IT roles are added to the generated roles' Permits or Requires list.
Entitlement Source Applications	Applications to mine for entitlements.
Percentage Threshold for Inclusion of an Entitlement	Specify the minimum inclusion threshold that an entitlement must meet before it is included in the role.

Use An Existing Business Role Mining Template

Use or edit an existing Business Role Mining template to generate a role based on previous criteria by clicking a template name in the Role Mining Templates panel on the Role Mining tab.

Click **View Latest Mining Results to view the results of the most recent mining task for this template**.

Any changes to the template are saved for this template unless the template name is changed. Once you have entered your criteria, click **Save** to save your selections, or click **Save and Execute** to save the template and run the role mining task. Executed mining tasks appear on the Role Mining Results tab.

Note: Names are required when creating role mining templates. When you edit an existing template, you are given the choice to either change the existing template or create a new template. If you create a new template you are require to give it a new name.

Role Mining Results

The Role Mining Results tab displays a table containing information about the role mining tasks run in IdentityIQ. Use the filtering tools to narrow down the viewable results by name, start / end date and result. Click a line item in the table to view the details of the mining result.

Right-click a line item to open a sub menu with different options depending on the role mining type. Business Role mining sub-menu options include View Results and Delete. IT Role Mining sub-menu options include View Results, Export to CSV, and Delete.

Table 12—Role Management - Role Mining Results Field Descriptions

Field Name	Description
Name	The name of the role mining template used for the task.
Date Complete	The date the role mining task completed.
Result	The result of the role mining task. Note: Click the refresh button at the bottom of the panel if the task status is "Pending". Right-click the task and select Delete to remove it from the Role Mining Results tab.
Owner	The identity named as owner of the role mining template.
Type	The type of role mining task.

Viewing the information and actions available on the role mining result details varies depending on the role mining type.

IT Role Mining Results Details

The IT Role Mining Results Details page displays a table containing a visual representation of the available unique roles generated based on the criteria used in the role mining task. Click a line item to highlight that row. Right-click the row to bring up a sub-menu from which you can select either View Group Summary, Create Role, or View Population. Click View List of Mining Results to return to the previous page.

Group Summary

The Group Summary window displays a quick view of the application and entitlements which make up that group.

Create Role

The Create Role window displays information about the role and its entitlements which were generated by the role mining task. Additional changes can be made here prior to committing to the role creation.

Table 13—IT Role Mining Results - Create Role Field Descriptions

Field Name	Description
Name	Input the name of the role being created.
Owner	The owner of the role being created.

Table 13—IT Role Mining Results - Create Role Field Descriptions

Field Name	Description
Scope	Select a scope from the drop-down list. Only scopes that you control are displayed in the list. Scope is used to determine the objects to which a user has access. If scoping is active, identities can only see objects that they created or that are within the scopes they control.
Container Role	Select a container role from the drop down list in which to have the created role placed.
Description	Enter a brief description of the role.
Direct Entitlements	Displays the entitlements that were mined as a result of the role mining criteria entered. Click the “X” icon to remove any entitlements. Note: No entitlements can be added. Entitlements can only be removed from the list. At least one entitlement must be included to successfully create a role.
Inherited Roles	Select from the drop-down list the roles, if any, in which this role is a member.
Entitlements from Inherited Roles	Displays the entitlements included in the inherited role. Click the “X” icon to remove any entitlements.

Click Save to complete the role creation or Cancel to close the window. The new role is available on the Role Viewer tab.

View Population

The View Population window displays information about the identities in IdentityIQ which match the criteria used by the role mining task. The information displayed in this table is defined when IdentityIQ is configured for your enterprise. By default the table displays Name, First Name, Last Name and Manager. Use the drop-down list at the top of the window to filter the results to display identities that match the criteria exclusively or those that match but have additional entitlements.

Business Role Mining Results Details

Click a Business Role Mining type line item to open the Latest Mining Results window for that mining task. The window displays detailed information on the roles generated based on the criteria used in the role mining task.

Table 14—Business Role Mining Results - Latest Mining Results Window Field Descriptions

Field Name	Description
Details	
Name	The name of the role which was created.
Type	The type of the role which was created.
Description	A brief description of the role which was created.
Status	Current status of the role mining task.
Started By	Displays the name of the person that launched the role mining task.

Table 14—Business Role Mining Results - Latest Mining Results Window Field Descriptions

Field Name	Description
Started	Displays the date and time on which the mining task was started.
Completed	Displays the date and time on which the mining task was completed.
Business Role Mining Attributes	
Attribute	Displays information regarding the following topics: Identity Mining attributes — attributes selected in the mining criteria. Roles mined — total number of roles mined based on the provided mining criteria. Roles updated — number of roles updated as a result of the latest mining task. Coverage of mined roles — displays the percentage of comparative roles used in the mining task based off of the mining criteria.

Working with the Role Manager

Use the following sections to work with roles in the Role Manager. These sections enable you to create and edit roles and profiles, perform role analysis, and approve new or modified roles.

- "How to Create or Edit a Role From the Role Management Page" on page 33
- "How to Create a Role From a Role Creation Request" on page 35
- "How to Create or Edit a Profile" on page 35
- "How to Approve Role Changes" on page 39
- "How to Perform Impact Analysis" on page 39

How to Create or Edit a Role From the Role Management Page

Use the following procedure to edit existing roles or create new roles. Roles can also be created from certifications and role mining.

Use the approval function to open approval work items for role owners. See "How to Approve Role Changes" on page 39.

Use the impact analysis function to create a report that provides details on the impact these changes can have on the rest of your product implementation. See "How to Perform Impact Analysis" on page 39.

Procedure

1. Access Role Management.
   Click **Setup > Roles**.
2. Click a role to edit.
   — OR —

   Select **Add** to create a new role.
3. Enter the role information. This information is used throughout the product.
   Name — A descriptive name of this role.

   Note: Role names with single quotation marks, double quotation marks, or commas are not supported.

   Type — The type of role being created. For example, organizational, business, or IT.
   Role type definitions are customizable and created as part of the configuration process.

Owner — The name of the owner for this role. Entering the first few letters of a name displays a select list of valid users and workgroups with names starting with those letters. Select a name from the list.

Description — A detailed description of the role.

4. *Optional:* Define activation events for the role being created.

   Note: Only one activation or deactivation event can be defined at a time.
   a. Click **Add Event** to display the Add New Event dialog.
   b. Manually enter a date or click the calendar icon to select a date.
   c. Select **Activate** or **Deactivate** from the **Action** drop-down list.
   d. Click **Save** to return to the Role Editor page.

   Select an event and click Delete to remove the event.

5. *Optional:* Define an assignment rule for the role being created.

   - **Match List** — define a list of entitlements to determine role assignment.
     For attributes select an attribute from the drop-down list and type a value.
     For permissions, type the name (target) and value (right).

   Note: If Null is selected, the associated value text box is disabled. When the is null match is processed, the term matches users on the chosen application who have a null value for that attribute/permission.

   - **Filter** — enter a custom XML database query to define user for this role.
   - **Script** — enter a custom script for role assignment. Scripts are similar to rules, but the source is stored with the role and can be edited from this page.
   - **Rule** — select an existing rule from the drop-down list.
   - **Population** — select a population from the list. Members of that population are assigned the role. Populations are generated as the results of identity searches.

6. *Optional:* Click **Modify Permitted Roles** in the Permitted Roles panel and modify the list of roles permitted by this role.
   a. Enter the first few letters of a role name in the **Select a role** field and select a role from the selection list.
   b. Click **Add** to add the role to the membership list.
      Add as many roles as required.
   c. Click **Save**.

7. *Optional:* Click **Modify Required Roles** in the Required Roles panel and modify the list of roles required by this role.
   a. Enter the first few letters of a role name in the **Select a role** field and select a role from the selection list.
   b. Click **Add** to add the role to the membership list.
      Add as many roles as required.
   c. Click **Save**.

8. *Optional:* Click **Modify Inheritance** in the Inherited Roles panel and modify the list of roles of which this role is a member. This role inherits entitlements from any role to which it is a member.
   a. Enter the first few letters of a role name in the **Select a role** field and select a role from the selection list.
   b. Click **Add** to add the role to the inheritance list.
      Add as many roles as required.
   c. Click **Save**.

9. Create new profiles or edit existing profiles from the Entitlements panel.
   Profiles created for this role are inherited by any role that is a member of this role.

10. Optional: Click **Add Provisioning Policy** in the Provisioning Policy panel.
11. Take one of the following actions:
    - Click **Submit** to save the role or, if the approval work flow is active, open an approval work item for the specified role owner.
      The approval feature is only available if the work flow was activated during configuration.
    - Click **Submit with Impact Analysis** to create a report that provides details on the impact these changes can have on the rest of your product implementation and open an approval work item if the approval work flow is active.
    - Click **Check Policy Conflicts** to display any policy violations created by changes made on this page. Policy checking is only available if impact analysis has been run.

Additional Information

To work with profiles associated with a role see:

- "How to Create or Edit a Profile" on page 35
- "How to Approve Role Changes" on page 39

How to Create a Role From a Role Creation Request

Use the following procedure to create roles from role creation request work items. Role creation request work items can be generated through the certification process.

Note: Approval is only required if the approval work flow is active. If approval is not required roles are added directly from the Create Role dialog.

Procedure

To create a new role from a role creation request, do the following:

1. Click the work item requesting the role in your inbox.
2. Review the information in the work item and do one of the following:
   - **Forward** — forward the work item to another authorized user to make the decision on the role. Optionally add comments on the **Forward Comments** dialog.
   - **Reject** — reject the proposed role. Optionally add comments on the Rejection Comments dialog.
   - **Approve** — continue with step 3 to proceed with the approval process.
3. *Optional:* Edit the name of the role.
4. *Optional*: Edit the owner of the role.
   Entering the first few letters of a name or workgroup displays a select list of valid IdentityIQ users and workgroups with names starting with those letters. Select a name from the list.
5. *Optional:* Edit or enter a description of the role being created.
6. Click **Approve** to display the **Approval Comments** dialog.
7. Add comments if they are required and click **Approve** to create this role.

How to Create or Edit a Profile

A profile is a set of entitlements on a specific application. An entitlement is either a specific value for an account attribute, most commonly group membership, or a permission. Profiles are specific to one role.

To Edit a Profile:

1. Access the Entitlement panel from the Role Editor page.
2. Edit the entitlement information.

   Note: If you change the application with which this profile is associated, all entitlements that you have created are removed.

3. Add or delete attribute rules and permissions.
   See "Role Editor - Edit Entitlement Panel" on page 18 for descriptions of the fields in each section.
4. Click **Save** to return to the Role Editor.

To Create a Profile:

- Create a new profile — See “How to Create a New Profile” on page 37.
- Create a profile using entitlement mining — “How to Create a Profile Using Entitlement Analysis” on page 36.

How to Create a Profile Using Entitlement Analysis

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

Entitlement analysis enables you to search for entitlements based on specific application and identity information. This feature enables you to create meaningful profiles without having to remember every entitlement on every application, or be familiar with the access assigned to each employee in your enterprise.

Entitlement mining also enables you to analyze the entitlement information collected to further refine the profiles you are creating before saving.

Procedure

Creating a profile using entitlement analysis actually involves three distinct phases:

- Searching for entitlements
- Analyze the search results
- Saving the profile

Search for Entitlements:

1. Access the Create Profile from Entitlement Analysis panel.
   Click **Create** in the Profiles panel of the Role Editor and select **New Profile From Entitlement**. Profiles can only be added within a role. See “How to Create or Edit a Role From the Role Management Page” on page 33.
2. Select the application on which to search for entitlements.
3. *Optional:* Narrow your entitlement search using the Identity Attribute fields.
   The Identity Attribute fields displayed are dependent on the identity attributes defined during configuration.
4. Click **Search** to begin the role analysis based on the specified criteria.

Analyze the Search Results:

The search returns the following information:

Note: The entitlement analysis search only returns those entitlements based on account or group attributes, not those based on permissions.

Table 15—Entitlement Mining Search Results Descriptions

Column	Description
Search Parameters:	
Attribute	The criteria used to define this search. For example, Application, Last Name, or Manager.
Filter Type	The type of filter applied to the search criteria. For example, Equal or Like.
Value	The value entered in the search field.
Only show percentages above: Use the slider to limit the results displayed in the table based on the percentage of the population to which the results apply. For example, if you are only interested in entitlements that apply to at least forty percent (40%) of the population searched, click the slider and move it to that percentage, or type the percentage in the field to the right.	
Entitlement Information: Click a value to display a list of all identities to whom that entitlement is assigned.	
Name	The name of the attribute from which this entitlement was derived. Attributes used to define entitlements are specified during configuration.
Value	The value assigned to the attribute. Click a value to expand a list of users to whom the entitlement is assigned.
Percent of Population	The number of identities assigned to that value of that attribute on this application expressed as a percentage of all identities that have an account on the application.

Use these results to analyze the entitlements that exist within your enterprise. The Group and Analyze feature enables you to group entitlements within an application and generate results based on that group. This feature enables you to see how assigning multiple entitlements to a profile can impact access within the application.

To group and analyze, select multiple entitlements and click **Group and Analyze**. The results are displayed below the entitlements table. Click a group to see the details for the entitlements within. You can perform analysis multiple times on entitlements or on the groups created.

Save the Profile:

When you are satisfied with the information you have mined and analyzed, click **Create Profile**. You must enter an name for the new profile, optionally a description, and click **Save** to return to the Role Editor.

Additional Information

From the Role Editor you can add additional profiles, edit the role or save the role and return to the Role Viewer. See “Role Editor Page” on page 15.

How to Create a New Profile

Use one of the following procedures to create a new profile.

P**rocedure 1**

Note: Click Simple View if you are in the advance view. The Simple View might not be available in all roles.

1. Click **Add** in the Entitlements Panel.

2. Select the application on which to apply this profile from the **Application** suggestion list.
   Enter the first few letters of an application name and select the application from the suggest list.
3. Select an account attribute and then an entitlement from the drop-down lists.
4. Click **Save** to return to the Role Editor.

Procedure 2

1. Click **Advanced View** in the Entitlements Panel.
2. Click **Create** in the Profiles panel of the Role Editor and select **New Profile**. Profiles can only be added within a role. See “How to Create or Edit a Role From the Role Management Page” on page 33.
3. Enter a description for the profile.
4. Select the application on which to apply this profile from the **Application** suggestion list.
   Enter the first few letters of an application name and select the application from the suggest list.
5. Add **Attribute Rules** and **Permissions** to the profile. To use the filter, see "Creating Attribute Rules" on page 38. For an explanation of the permission options, see "Creating Attribute Permissions" on page 38.
6. Click **Save** to return to the Role Editor.

Additional Information

From the Role Editor you can add additional profiles, edit the role or save the role and return to the Role Modeler page. See “Role Editor Page” on page 15.

Creating Attribute Rules

Use the Attribute Rules function to add and combine filters to define your profiles. Apply qualifiers to attributes within filters to limit the values returned and then use grouping and AND\OR operations to create the rules that make up the profile.

Add a Filter:

Create the filters that make up the attribute rules.

- **Field** — select an attribute value from the drop-down list. This list contains all of the attributes mapped from the selected application.
- **Search Type** — the qualifier to associate with the value, for example equals or like.
- **Value** — the value of the attribute.
- **Ignore Case** — specifies if case should be factored into the query.

Filter(s):

The Operations drop-down list enables you to specify AND/OR relationships between the filters in the list. You can use multiple layers of filter grouping containing AND\OR operations to create complex attribute rules. For example, you can create an attribute rule that returns all users who are in payroll OR human resource AND located in Chicago.

Creating Attribute Permissions

Use the permissions panel to add permissions to the profile. Permissions define rights on targets on the application. Select rights from the rights lists (for example, create, read, update, delete, execute), and specify the target attribute in the Target field. Use the Shift and Ctrl keys to select multiple rights.

How to Approve Role Changes

When roles are created or edited, they might require approval from the designated owner before they become active. Work items are created and sent to the owners when approval is necessary. Use this procedure to review and approve or reject role changes.

Role analysis and role approval are an important part of the overall role life-cycle management. Role analytics and approval, both for new or modified roles are controlled thought business processes configured for your implementation of IdentityIQ.

Procedure

1. Click an approval work item in your Inbox on the to display the Approval page.
2. Review the summary information of the work item.
3. Review the comments associate with the work item and, optionally, add comments.
4. Review the details sections.
   Modification approvals — review the changes in the Modified Role or Modified Profile table and make a decision.

   Creation approvals — review the information in the New Role or New Profile panel, make the necessary modifications, and make a decision. Some of the information is read only**.**
5. Click **Review Pending Changes** to display the Role Editor and review the changes proposed for the role.
6. Make a decision.
   Approve — approve the creation or modification. Add comments if needed and confirm the approve on the Approval Comments dialog.

   Reject — reject the request for approval on the creation or modification. Add comments if needed and confirm the rejection on the Rejection Comments dialog.

   Forward — forward the approval work item to another user. Entering the first few letters of a name displays a select list of valid users with names starting with those letters. Select a name from the list. Add comments if needed.

   Cancel — cancel the work you have done on the work item.

How to Perform Impact Analysis

Use the impact analysis function to create a report that provides details on the impact these changes can have on the rest of your product implementation.

When you click the **Submit with Impact Analysis** from the Role Editor, the changes are rolled into a work item that is assigned to you, an analysis task is launched, and a link is created inside the work item that points to the task results. You can navigate from the work item to the task result to check on the status of the task as it is running.

Impact analysis can also be performed from the Task page using the Role Overlap Analysis tasks. Overlap analysis returns information on the following overlap facets:

- Attributes — overlap between extended attributes and a some system attributes
- Local Assignment — overlap between assignment rules and profiles defined directly on the role (not inherited)
- Hierarchal Assignment — overlap between both local and inherited assignment rules and profiles
- Local Provisioning — overlap between provisioning side effects defined directly on the role
- Hierarchical Provisioning — overlap between both local and inherited provisioning side effects

Note: The Assignment and Provisioning numbers are the same for simple roles. However, the numbers are different when there are manually written provisioning plans. The numbers are also different when the profiles use OR terms because provisioning only picks the first terms using OR.

Procedure

1. Click an impact analysis work item in your inbox to open the Role Approval page.
2. Review the summary information of the work item.
3. Review the comments associated with the work item and, optionally, add comments.
4. Review the details of the changes being analyzed by the impact analysis task associated with the work item.
5. Click **Click to view analysis task results** to display the task results page containing the actual impact information obtained by the task.
6. Review the impact information and click **Return to Work Item** to return to the work item and make a decision on the request.
7. Make a decision.
   Approve — apply the creation or modification based on the content of the impact analysis task results.
   Reject — discard any changes made to the role based on the impact analysis results.
   Forward — forward the impact analysis work item to another user. Entering the first few letters of a name displays a select list of valid users with names starting with those letters. Select a name from the list. Add comments if needed.
   Cancel — cancel the work you have done on the work item**.**

Multiple Role and Account Assignment

IdentityIQ allows roles to be assigned to an identity more than once and applied to different sets of accounts associated with the identity. A second feature allows a role assignment to apply to multiple accounts on the same application.

Multiple Role Assignment

A system and a role-specific option allows a role to be assigned to an identity more than once and have the associated entitlements apply to different accounts.

The model that is used to persist role assignment on an identity includes the accounts to which the role assignment is provisioned. This model is referred to as target account memory. The role assignment can also contain an assignment note that describes why the assignment exists. The assignment note is useful for

differentiating multiple assignments. For example, you can have one assignment with a note of Standard Account and a second assignment with a note of Privileged Account.

When a role is assigned, the applicable accounts are selected automatically using rules or through an interactive user interface. The selection of accounts can optionally be a directive to create a new account. Account selection rules can be defined on a role that can contain entitlements that can be provisioned from profiles to automate the selection of applicable accounts. There can be a general rule for the role as well as a rule for every application included in the role profiles.

For Lifecycle Manager access requests, the requestor is prompted, if they are required by the configuration settings, to select the accounts to use for the request. This occurs if multiple accounts already exist on the relevant applications or IdentityIQ is configured to allow a new account to be created and account selection rules did not automatically select the appropriate accounts. The requestor can enter an assignment note during account selection.

When role assignment rules are processed during the Identity Refresh task, the default behavior is to skip any role provisioning that does not explicitly define the target account and to report the number of times provisioning was skipped. The Identity Refresh task can be configured to create required account selection work items if appropriate account selection rules are not defined, but care should be to be taken to ensure that this does not create an inordinate number of work items. To prevent the need for manual interaction, the best practice is to have completely defined account selection rules for all profiles associated with rule-based role assignments where multiple role assignment is allowed.

Details about the accounts that an assigned role applies to and the optional assignment note are displayed in the appropriate user interfaces including: Entitlements tab of the View Identity page, Certifications pages, Lifecycle Manager Current Access, Lifecycle Manager approval work items, and Manage Access Request details. Additionally, these user interfaces have a role listed multiple times if the role is assigned more than once.

Multiple Application Accounts in an Assignment

In a standard role assignment, a role can provision to no more than one account on a specific application. If the role hierarchy contains more than one role that targets the same application, the entitlements for the assigned role are all provisioned on the same account.

An option can be specified on any role that can be contained on a permitted or required list of another role, or any role that contains entitlements that can be provisioned from profiles or any role that contains a provisioning policy, that allows the entitlements in that role to be provisioned to a selected account or to a newly created account. If there is more than one role that can be provisioned that uses this option in the assigned role hierarchy, a different target account (including creating a new account) can be selected for each role.

Role Detection

All detected roles store information about the accounts and entitlements that fulfilled the detection. Detection recognizes and persists if a detected role was part of an assignment. For example, explicitly requested in a Lifecycle Manager access request.

A role can be detected more than once if there are role assignments targeting different accounts on the same application. For example, if assigned role A and assigned role B both have required role R, but different target accounts were selected for A and B, there are two detections of R. One for the accounts selected for A and one for the accounts selected for B. This model is necessary to accurately show which accounts and entitlements are included in each role assignment.

Hard and Soft Permitted Roles

A **hard permitted role** is a role that is requested through IdentityIQ. A **soft permitted role** is a role that is discovered through aggregation and entitlement correlation, but was not explicitly requested or provisioned using IdentityIQ.

When a role that contains hard permitted roles is unassigned and de-provisioned, the hard permitted roles is also de-provisioned if there are no other dependencies on those roles. If a role containing soft permitted roles is unassigned and de-provisioned, the soft permitted roles are not de-provisioned.

Identity Role Assignments

Role assignments have an assignment id that is used to uniquely refer to the assignment. The user interface does not display this assignment id, but any code that references an assignment needs to use the id to keep a reference from being ambiguous.

When a permitted role is requested through Lifecycle Manager, IdentityIQ records the request in the RoleAssignment model by placing a nested RoleAssignment for the permitted role inside the RoleAssignment for the assigned role. This process defines a hard permitted role.

The identity assignedRoles and assignedBundleSummary attributes are a unique list of roles, and if a role is assigned multiple times, the role is in this list only one time. The identity roleAssignments attribute can contain multiple items for the same role if the role is assigned multiple times.

Existing methods on the identity object related to role assignments remain for backward compatibility, but are marked deprecated and can return incomplete results if multiple assignments are enabled.

Provisioning Plans

If multiple assignments are enabled and exist, a provisioning plan to modify assignments must specify an assignment id to prevent ambiguity. When an assignment is being added and the intention is to create a second assignment, a special assignment id token of new is used.

A single attribute request can contain a list of roles that are to have their assignments changed. When multiple assignments are enabled and exist, each role must be contained in a separate attribute request so that an assignment id can be specified.

The provisioner remains backward compatible and continues to process provisioning plans without assignment ids or role lists.

If multiple assignments are enabled, it is imperative that provisioning plans are well formed and include the correct data to impact the desired change.

When multiple assignments for the role exist, a provisioning plan that includes a request to remove a role assignment by name without an assignment id removes one indeterminate role assignment. When an assignment for a role already exists, a provisioning plan that includes a request to add a role assignment without an assignment id or a new token selects one indeterminate role assignment and provision any missing entitlements.

Automated Propagation of Role Changes to Role Members

When managing role model in IdentityIQ any changes to the role or delete a role, would propagate to all identities that are currently assigned to the said role. This allows you to use role model as a true authoritative source for requested access. To allow propagation of role changes, you must set a configuration flag in System Setup.

If the above flag is set, role changes are provisioned. Change propagates to all identities that have that role and any revokes or additions that need to take place occurs. Examples of role changes include:

- role requirements changes, such as adding or removing an entitlement
- role Inheritance changes, such as disabling or enabling role
- changes to the list of required roles are needed

Propagation of changes are set to a **RoleChangeEvent** table and picked up by **Propagate Role Changes** task based on a created time.

Note: When a role is deleted, it is marked for deletion and the user is unable to make edits to the role. When a role is deleted, all entitlements assigned to that role are deleted.

Chapter 3: Group and Population User Interface

Use the Group Configuration page to work with groups and populations within your enterprise. When these items are enabled, you can track and monitor activity by membership and risk information.

To access the Group Configuration page, select **Setup -> Groups** from the navigation bar.

Note: Group management is an advance process that requires the assignment of addition IdentityIQ capabilities before these pages are displayed.

The Group Configuration page has the following tabs:

- "Group Tab" on page 46 — Groups are defined automatically by values assigned to identity attributes such as Department, Location, Manager and Organization, or are based on common entitlements within an application, not common qualities as defined within IdentityIQ.
- "Populations Tab" on page 47 — 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. Because population membership is based entirely on identity search parameters, members do not have to share the same identity of account group membership.
- "Workgroups Tab" on page 49 — Workgroups enable the assignment of object ownership, certification, revocations and work items to pre-defined lists of identities. You can also 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.

Group Examples

Groups Associated with Identity Attributes

Groups associated with identity attribute values are defined by the values assigned to those attributes. For example, the Location identity attribute might 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 containing the identities that have the corresponding value assigned to Department.

Groups Based on Common Entitlements

Groups based on common entitlements within an application are defined by shared access and are listed under role. An entitlement is either a specific value for an account attribute or a permission. A role is a collection of entitlements that enable an identity to perform certain operations within your enterprise. When the role group attribute is created and enabled, each role becomes a group consisting of all identities that share the entitlements that make up that role. Identities assigned entitlements that do not combine to match the criteria of a role are

assigned to the group No role. Th Global group contains all identities.

Group Tab

The Groups table contains a list of the high-level containers, or group factories, that contain the actual groups used within IdentityIQ. Each group factory is associated with either an identity attribute or an entitlement within an application. These group factories are not groups themselves, but are used to define, maintain, and enable groups.

The Group tab contains the following information:

Table 16—Groups Tab Column Descriptions

Column Name	Description
Name	The name assigned to the group factory when it was created.
Attribute	The attribute used to define the groups within the group factory.
Description	Description of the group factory or the groups contained within.
Status	The status of the groups within the group factory, enable (check mark) or disabled (exclamation mark). This status controls all of the groups contained within this group factory.

Click on a group factory or right-click and select edit to display the Edit Group page. The Edit Group page contains the group factory information from the table and a list of the groups associated with the group factory. For example, for a Manager group factory the table contains a row for every value assigned to the manager attribute in IdentityIQ. See “Edit Group Page” on page 46.

To create a new group, click **Create New Group** to open the Edit Group page.

To delete a group factory, right-click and select **Delete**.

Edit Group Page

This page is used to enable or disable all of the groups contained within a group factory, recreate a group factory that has been deleted, and view the groups that make up a group factory. Creating multiple group factories of the same type produces identical results when a task is run that updates group information. For example, if you create three (3) group factories, X, Y, and Z and specify the Department attribute for each, you receive identical results for all three group factories when you run a task that updates group information.

The Edit Group page contains the following information:

Table 17—Edit Groups Column Descriptions

Column Name	Description
Group Information:	
Name	The name assigned to the group factory when it was created.
Group Attribute	The attribute used to define the groups within the group factory.
Description	Description of the group factory or the groups contained within.

Table 17—Edit Groups Column Descriptions

Column Name	Description
Enabled/Disabled	The status of the groups within the group factory, **Enabled** or **Disabled**. This status controls all of the groups contained within this group factory. **Enable** — the groups are active and available for use and activity searching. **Disabled** — the groups exist, but are not included in statistical tracking or available on the search pages.
Scope	The scope for this group factory. If scope is assigned, only the users that control the designated scope can see this group factory in select lists on pages such as the Certification Schedule or Search pages. The sub-groups associated with this application are visible to a user with any or no controlled scope. Depending on configuration settings, objects with no scope assigned might be visible to all users with the correct capabilities.
Sub-Group Information: **Note: This information is not displayed until group aggregation is performed by a task. See "Tasks" on page 283.**	
Name	The name of the group, or the value assigned to the specified attribute.
Member Count	The number of identities matching the group criteria.
Policy Violations	The total number of policy violations for members of the group.
Composite Score	The average composite risk scores of each member of the group.
Owner	The owner of the sub-group, if one is assigned.
Last Updated	The last time a task was run that updated the group information.

Populations Tab

The Populations tab contains a list of populations that either you created from identity searches or that were created by other users and defined as public. 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.

The Populations tab contains the following information:

Table 18—Populations Tab Column Descriptions

Column Name	Description
Name	The name assigned to the population when it was created.
Description	Description of the population.

Table 18—Populations Tab Column Descriptions

Column Name	Description
Visibility	If the population is Private or Public. **Private** — only visible to the user that created them. **Public** — available to any user with access to pages on which they are used and control of the correct scope, if scoping is active.
Owner	The name of the population owner, if one is assigned.
Status	The status of the population, enable (check mark) or disabled (exclamation mark). **Enable** — the populations are active and available for use in activity searching. **Disabled** — the populations exist, but are not included in statistical tracking or available on the search pages.

Click on a population or right-click and select edit to display the Edit Population page. The Edit Population page contains the population information and a list of associated identities. See “Edit Population Page” on page 48.

To delete a population, right-click and select **Delete**.

Edit Population Page

This page is used to edit population information, enable or disable populations, mark populations as private or public, set the scope for the population, and view the identities that make up a population.

Note: Any user that has access to a public population can make changes on that population.

Note: If you mark a public population as private, and you are not the creator of that population, you can no longer see that population.

Click on an identity to display the View Identity page for that user.

That Edit Population page contains the following information:

Table 19—Edit Populations Column Descriptions

Column Name	Description
Group Information:	
Name	The name assigned to the population when it was created.
Description	Description of the population.
Private	Select or clear the check-box to specify if the population is private or not private. **Private** — only visible to the user that created it from the search results page. **Not Private** — available to any user with access to pages on which they are used and control of the correct scope, if scoping is active.
Enabled/Disabled	Select or clear the check-box to specify if the population enabled or not enabled. **Enable** — the populations are active and available for use inactivity searching. **Not Enabled** — the populations exist, but are not included in statistical tracking or available on the search pages.

Table 19—Edit Populations Column Descriptions

Column Name	Description
Scope	The scope for this population. If scope is assigned, only the users that control the designated scope see this population in select lists on pages such as the Certification Schedule or Search pages. This scope only applies to the population, not the identities contained within.
Owner	Assign an owner for the population.
Population Information:	
Population Count	The number of identities in IdentityIQ matching the populations search criteria.
Name	The value of the accountId attribute for the identity.
First Name	The value of the firstname attribute for the identity.
Last Name	The value of the lastname attribute for the identity.
Manager	The value of the manager attribute for the identity.
Last Refresh	The date on which the identity was last refreshed.

Workgroups Tab

The Workroups tab contains a list of 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.

The Workgroups tab contains the following information:

Table 20—Workgroups Tab Column Descriptions

Column Name	Description
Name	The name assigned to the workgroups.
Description	A short description of the workgroup.
Modified	The date and time the workgroup was last modified.

Click on a workgroup or right-click and select edit to display the Edit Workgroup page. The Edit Workgroup page contains the group information and a list of capabilities and members. See “Edit Workgroups Page” on page 49.

To create a new workgroup, click **Create Workgroup** to open the Edit Workgroup page.

To delete a workgroup from the list, right-click and select **Delete**.

Edit Workgroups Page

This page is used to edit workgroup information and view the capabilities, scope and members that make up a group.

That Edit Workgroup page contains the following information:

Table 21—Edit Account Groups Column Descriptions

Column Name	Description
Group Information:	
Name	The name assigned to the workgroup.
Owner	The owner assigned to this group.
Description	Description of the group.
Scope	The scope for this workgroup. If scope is assigned, only the users that control the designated scope can see this workgroup in select lists on pages such as the Certification Schedule or Search pages. This scope only applies to the workgroup, not the capabilities or identities contained within.
Group Email	Specify the email address assigned to this workgroup. A workgroup email address should be a distribution list. If no address is specified here, notifications are sent to each member of the group. **Note: A workgroup email account needs to be created in your email system.**
Notification Setting	Specify to whom notifications should be delivered. **Note: If you select Notify members and group email and the group email is a distribution list, the members receive the notification twice.** **Notify members and group email** - send notifications to each group member and the group email address. **Notify group email only** - send notifications to the group email address but not the individual group members. **Notify members only** - send notifications to each group member, but not the group email address. **Disable notifications** - send no notifications to this group. This restriction only applies to items assigned to the workgroup.
Rights:	
Capabilities	The SailPoint capabilities available. The capabilities currently assigned to the workgroup are highlighted on the list. **Note: Each member of the group assumes the capabilities of the group, even if different capabilities were assigned to them individually.** Use the Ctrl and Shift keys to select multiple capabilities.

Table 21—Edit Account Groups Column Descriptions

Column Name	Description
Authorized Scope	The scopes controlled by this workgroup. Scope is used to determine the objects to which the members of this group have access. Control determines access. If scoping is active, the workgroup members can only see objects that are within the scopes controlled by the group. Assign scopes to the workgroup using the suggestion field at the top of the Authorized Scopes list box. - Click the arrow to the right of the suggestion field to display a list of all scopes defined. - Enter a few letters in the suggestion 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. See “Scopes” on page 47
Can Access Assigned Scope	Select this option to enable the workgroup members to control the scope to which they are assigned. If this option is cleared, the users do not have access to objects within the scope to which the workgroup is assigned. Control determines access. If scoping is active, identities can only see objects that are within the scopes they control.
Members: The list of members of the workgroup. Use the drop-down list at the bottom of the table to select identities and the click **Add Member** to add members to the workgroup. Use the select boxes to select members and click **Remove Members** to remove members from the workgroup.	