IdentityIQ Role, Group, and Population Management

Version: 8.4

Revised: September 2023

Copyright and Trademark Notices

Contents

Introduction to Roles, Workgroups, Populations, and Groups

IdentityIQ offers several ways to group Identities into sets, based on shared characteristics. Each type of grouping has a distinct purpose and offers unique capabilities. They include:

Roles

Roles model the organization's job functions, structure, and system entitlements, and present entitlement data in a way that is readily understood by non-technical reviewers . Through roles, entitlements can be grouped together and presented as a logical unit, such as a job function, rather than as a detailed and often difficult-to-interpret list of access rights.

Workgroups

Workgroups associate sets of Identities to make it possible to share responsibilities within IdentityIQ ; these responsibilities can include certification access reviews and ownership of application entitlements, among others.

Populations

Populations are query-generated lists of Identities that share a common set of attributes, such as location, department, risk score, et cetera; populations can be used to filter the set of identities that are included in a certification, task, or report.

Groups

Groups are sets of Identities created based on the value of a single identity attribute; groups can be used to filter the set of identities that are included in a certification, task, or report.

Roles

IdentityIQ roles are used to model a company's structure and business operations. Roles are designed to be highly flexible and can be customized 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; typically do not perform any function other than creating a nesting structure in the Role Modeler.

Business

Identify job functions or titles, or other attributes by which users can be grouped together.

IT

Encapsulate sets of system entitlements from one or more applications to be grouped together into a single role. IT roles should encapsulate groups of related entitlements that are shared by one or more business roles.

Entitlement

Represent individual system entitlements; entitlement roles were originally created to represent a single entitlement on a single application; currently, Entitlement Roles exist for backward compatibility with versions 5.x and earlier of IdentityIQ, and are not recommended for current/new installations.

Custom Role types can be created to model a structure that does not 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.

Role Management

IdentityIQ provides robust role management features that helps customers to implement an enterprise role model, to simplify compliance and provisioning processes for line-of-business users. It helps enterprises align low-level IT privileges with their corporate structure and business operations by grouping individual entitlements into higher-level business functions, and it abstracts business users from the underlying complexity of IT authorization models.

The sections here will help you learn how to build and manage a robust role model in IdentityIQ.

Role Management Concepts — Important terms and concepts to help you understand how best to use IdentityIQ's role management features

Global Configuration and Settings for Roles —Global Configuration and Settings for RolesSet global configurations and global defaults for roles and role behavior.

Role Modeling — Create and maintain the roles that define your enterprise.

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.

Automated Propagation of Role Changes to Role Members — When a role is changed or deleted, that change propagates to all identities that are currently assigned to the role.

Role Management Concepts

The sections below outline some important terms and concepts regarding roles and how they are managed in IdentityIQ.

- Benefits of Roles
- Role Types
- IdentityIQ's Two-Tier Role Model
- Linking IT Roles to Business Roles: Required and Permitted Access
- Role Inheritance
- How Roles are Created
- How Roles are Assigned
- Reviewing and Monitoring Roles and Role Assignments
- Role Based Access Control (RBAC)

Benefits of Roles

A major benefit of implementing roles is using them to translate entitlement data into terms that can be more clearly understood by business managers and other employees, as they request, assign, and review access. Through roles, entitlements can be grouped together and presented as a logical unit, such as a job function, rather than as a detailed and often difficult-to-interpret list of access rights.

In some cases, the way entitlements are named or described can make it difficult for a reviewer to understand what the entitlement means. For example, groups names may use acronyms or numeric values which do not offer a great deal of contextual information to the layperson; even when names are more descriptive, inclusion of DN data in the group name may obscure the important values, at least at first glance. Roles can be used to simplify and clarify how the data is presented to the business user.

Sometimes a single job function may require multiple system entitlements, either all on the same application, or across multiple resources. Without roles, the reviewing manager needs to know about all of the required pieces – both to understand why an employee has access to each of these, and to ensure that employees have all the access they need to do the job. With roles, all of these permissions can be encapsulated in a single role and presented to the reviewer as a unit, both clarifying and simplifying the reviewing process.

Similarly, encapsulating entitlements into roles also makes it possible for a manager to automatically provision the required entitlements for a new employee, simply by assigning that person the appropriate role.

Role Types

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

Organizational Roles

Organizational roles are designed for organizing the role hierarchy in the IdentityIQ UI for easier management. By default, they do not perform any function other than creating a nesting structure in the Role Modeler. Organizational roles can be defined in any hierarchical structure desired. Possible structures could include:

- A hierarchy matching the corporate org structure for organizing business roles into easily managed groupings
- A set of container roles for holding collections of IT roles based on commonalities between them
- A set of container roles grouping other roles by application
- A set of container roles grouping other roles alphabetically
- Any combination of these structures (or others)

The key is to use organizational roles to simplify navigation through the role structure for administrators who will be tasked with managing the roles.

Business Roles

Business roles generally represent job functions, titles, or responsibilities. They are usually tied to the organizational structure and are assigned to users based on their functions in the business – such as “Treasury Analyst” or “Accounts Payable Clerk”. Business roles define the **desired** state for a user’s access: what do you want someone with this job function to be able to do, or not do?

For example, within the Accounts Payable department, there might be an AP Supervisor, 3 AP Lead Accountants, and 30 Accounting Clerks. This would require the creation of 3 business roles:

- AP Supervisor
- AP Lead Accountant
- AP Clerk

However, if all clerks don't do the same basic job, it may help to create additional roles to further divide them into sub-units. For example, perhaps the mailroom clerks are tasked with opening, stamping, and digitally scanning invoices while other clerks are responsible for accounting system data entry and reporting. In that case, the department might implement four business roles:

- AP Supervisor
- AP Lead Accountant
- AP Entry Clerk
- AP Mailroom Clerk

In some cases, business roles may be defined by the managerial hierarchy in place at the company. For example, there may be a strict hierarchy of managerial and supervisory job titles that is replicated within any division or department, such as

- Vice President
- Director
- Manager
- Supervisor
- Lead

Business roles are assigned to users directly, either automatically via attribute matching on things like job title or department, or via request, which may come from the user himself or from someone else, like a manager or an application owner.

IT Roles

IT Roles encapsulate sets of system entitlements. They are tied to actual permissions within an application or target system. IT roles represent the **actual** state of the user's access, such as an account, entitlement, or permission. IT roles should encapsulate groups of related entitlements that are shared by one or more business roles. If too many entitlements are grouped together, each IT role may only apply to one business role and lose any potential reuse

benefits. If too few are grouped into each IT role, each business role will have to be connected to large numbers of IT roles to provide the required system access for the job; this can also result in role proliferation that makes role management an overly cumbersome activity, reducing their value to the organization. The goal therefore is to encapsulate as many entitlements into each role as possible without over-grouping.

A user's IT roles can be detected in IdentityIQ based on the entitlements that user has. Access can also be provisioned in IdentityIQ through IT roles.

Entitlement

Entitlement roles were originally created to represent a single entitlement on a single application; currently, Entitlement Roles exist for backward compatibility with versions 5.x and earlier of IdentityIQ, and are not recommended for current/new installations.

Custom Roles

Custom role types can be created to model a structure that doesn't easily fit into the IdentityIQ default model. In addition, existing role types can be configured to function differently from their default behaviors. Because there are so many ways roles can be customized, this document only discusses IdentityIQ's role structure in the default configuration.

IdentityIQ's Two-Tier Role Model

IdentityIQ by default uses a two-tier role model, to facilitate matching a user's business responsibilities to their actual access. Although you are not required to implement your roles using this two-tier model, it is helpful to understand the benefit of this model as you plan your implementation.

In the two-tier model, IT roles are *linked* to business roles, to tie actual access to your defined job functions and titles. This allows end users such as managers or access reviewers to work with familiar, user-friendly business roles rather than having to understand and act on every individual entitlement that is managed in IdentityIQ. IT roles can be shared by multiple business roles, as needed.

Linking IT Roles to Business Roles: Required and Permitted Access

When IT roles are linked to business roles, IdentityIQ uses the IT role definitions to know what access it should provision for a user when they are assigned the business role. Business roles and IT roles are linked using two types of relationships: required and permitted.

IT roles are connected to business roles through the **Required Roles** and **Permitted Roles** lists.

- **Required** roles refer to the set of access that someone with a given role **must** have. Someone with an Accounts Payable business role, for example, will always need have to have read and write access to the

accounting system.

- **Permitted** roles mean the access is discretionary – these are permissions or entitlements a user **may be allowed to have, but isn't required to have**. When permitted access is included with a business role, the entitlements are essentially "pre-screened" – we know that a user with this role is allowed to have the permitted access. For example, perhaps all employees are allowed to have VPN access but aren't automatically given this access unless they or their manager requests it.

The required IT role connection is used as the driving force for provisioning entitlements based on role assignment. When a business role is assigned to an Identity, requiring entitlements the Identity does not have, the entitlements for the required IT roles will be provisioned for the Identity. Depending on how provisioning is configured, this process can range from entirely manual to fully automated.

These require and permitted connections also help identify missing entitlements during the certification process. When a user is missing required entitlements for the IT roles under business roles assigned to them, the access review can reflect this to bring it to the reviewer's attention. Correction of that state is not done in the certification process itself; that is left to the refresh process or some other out-of-band process.

Role Inheritance

In some organizations, business roles or IT roles can be efficiently modeled using an inheritance-based role structure.

Business roles

Business roles can be modeled with inheritance when a set of business roles can be defined by increasingly specific criteria. Consider a Help Desk team made up of three support levels (business roles). Each higher numbered level may be able to do all the same activities as the lower numbered group(s) but also have extra tasks that the lower numbered groups do not do.

For example:

Help Desk Level 1

- Answer calls, troubleshoot basic issues
- Route complex problems to Level 2

Help Desk Level 2

- Diagnose problems routed from Level 1
- Refer problems not resolved within 24 hours to Level 3
- Answer calls and engage in basic troubleshooting when time available

Help Desk Level 3

- Resolve problems referred from Level 2
- Assist with Level 2 issues when time available
- Answer calls and engage in basic troubleshooting when time available

Perhaps the organization is structured so that all Help Desk personnel are assigned to the Department “Help Desk”. Additionally, all Level 2 and Level 3 Help Desk personnel are in the Denver location (while Level 1 personnel are not). Further, Level 3 personnel must hold the job title “Senior Engineer.”

These increasingly-specific shared attributes can be used to create the assignment rules for each of the inherited roles. When IdentityIQ applies the assignment rules to an inherited role structure, the role assigned to each Identity is the deepest one in the inheritance hierarchy that applies.

When the assignment rules run, Identities are assigned to only one of the roles in an inheritance structure. Only the most specific role – the deepest level in the hierarchy – that applies to the Identity is assigned. In other words, if an Identity’s attributes meet the criteria for Level 1 and Level 2, Level 2 is assigned; if they match all three Levels’ criteria, Level 3 is assigned.

IT roles

IT roles are modeled with inheritance when entitlement access for one set of Identities is a superset of the access grant to another set of Identities. For example, perhaps all Engineering users have access to the bug tracking system and project planning tool, but only Developers have access to the version control system. The Developer IT role could inherit from the Engineering IT role. Detection of IT roles in an inheritance structure operates on the same basic premise as assignment of inheritance-based business roles: an Identity will only have one role in the hierarchy detected for it and it will be the deepest one that applies to that Identity. In the Engineering example, an Identity that has the Developer IT role detected for it will not also have the Engineering IT role detected. However, the Developer IT role is only detected if all entitlements for both roles are found on the Identity.

Limitations of Role Inheritance

It is important to note that if organizational roles are interspersed with business roles in a hierarchy, the organizational roles’ presence will disrupt the inheritance functionality. Inheritance of these traits only applies to roles of the same type that inherit from each other in a hierarchy that is not interrupted by other role types.

The direct inheritance of an IT role directly in a Business or Container role is not supported.

Understanding Relationships Between Roles and Entitlements/Permissions

Roles bundle sets of access (entitlements and permissions) together so that access can be more easily managed and governed. **Entitlements**, which typically take the form of an account on an application or membership in a group,

control access to a system or application, and encompass actions the user with the entitlement can take in the application. **Permissions** represent direct access, independent of account or group membership, to an action a user can take in a system or application.

The access allowed by roles can be **direct** or **indirect**. For example, an Accountant role can give *direct* access to the Accounting system, in the form of an account on the system. *Indirect* access is typically granted through nested groups or a set of inherited roles; for example, an Accounting Supervisor role may inherit the Accountant role, and thereby be indirectly granted all the access an Accountant would have on the Accounting system.

Part of maintaining an efficient and functional role model is understanding and monitoring the connections between roles and the entitlements and permissions they allow.

For example, if you are making changes to the set of entitlements defined in your Active Directory application, it's important to understand which roles will be affected by those changes. Or, if you want to examine your role model to see where different roles may overlap in terms of the access they grant, it's useful to be able to see exactly which entitlements and permissions are included within multiple roles. If an application is going to be retired, it's useful to review ahead of time which roles include access to the application, so that the role can be changed accordingly.

IdentityIQ provides many tools to help you monitor and manage the relationships between roles and entitlements/permissions. You can examine roles to discover which entitlements and permissions they grant, and you can also examine entitlements and permissions to see which roles include them.

Establishing Connections Between Roles and Access

An IdentityIQ task called **Role-Entitlement Associations** builds a table of relationships between roles and access, ensuring referential integrity in your role model. This task only needs to be run one time to establish role associations to entitlements and permissions; once it has been run, IdentityIQ automatically updates the relationship table any time changes are made to role profiles.

This task is run by default when upgrading from an earlier version of IdentityIQ to the current version; in an upgrade scenario, you do not need to run the task independently of the upgrade process in order to establish these relationships.

Although there is no requirement to run the Role-Entitlement Associations task again after it is first run, you can choose to run it if you want to – for example, if you have onboarded many applications in a short timeframe and want to take extra care to ensure that your relationship table is up to date.

Examining Roles: What Access Do They Provide?

The **Role Profiles Composition** report lets you see which entitlements and permissions are included in specific roles. See the IdentityIQ **Roles** documentation.

The **Advanced Analytics** Role search includes criteria to search for roles by access profile, for entitlements, permissions, or both. See the IdentityIQ **Search** documentation.

The **Role Viewer** (**Setup > Roles**) lets you drill into Role Statistics details about individual entitlements; the detail view lists Associated Roles where relevant. See The Role Viewer Tab.

Examining Entitlements and Permissions: Which Roles Include Them?

The **Roles by Entitlement** report lists all roles that grant particular entitlements or permissions. See the IdentityIQ **Reports** documentation.

The **Role Member** report includes entitlement and permission criteria, that lets you see which users are members of roles that grant specific access. See the IdentityIQ **Reports** documentation.

The **Advanced Analytics** Role search includes criteria to search for roles by access profile, for entitlements, permissions, or both. See the IdentityIQ **Search** documentation.

You can drill down to **Role Association** information for entitlements and permissions in these areas of IdentityIQ:

- The **Entitlement Catalog** includes an Associated Roles tab listing the roles that provide direct access to the entitlement. See the IdentityIQ **Application Management** documentation.
- In the **Identity Warehouse**, you can click on individual entitlements to see Associated Roles that provide direct access to the entitlement for this user. See the IdentityIQ **Identity Management** documentation.
- In the **Application Definition**, the **Accounts** tab for the application lists users with accounts on the application. You can click the arrow next to a user to see specific entitlements, then click on an entitlement to see details that include Associated Roles where applicable. See the IdentityIQ **Application Configuration** documentation.
- **Work items** for access review challenges or decisions include an option to drill down into specific entitlements to see Associated Roles where applicable. See the IdentityIQ **Work Items** documentation.
- In **Targeted Certifications**, the **What do you want to certify?** section lets you enter criteria for selecting roles. Source Application, Source Attribute, and Source Value filtering attributes let you refine which roles are included in the certification by the entitlement access granted by the roles. See the IdentityIQ **Certifications and Access Reviews** documentation.
- When adding or removing access using the **Manage User Access** Quicklink, you can filter access based on the Role Source Application, Role Source Attribute, or Role Source value. You can also click the **Details** button on access items and drill down into the **Entitlement Profile** to see Associated Roles for the item.
- When approving access, you can click the information icon (?) for any access item, and drill down into the **Role Hierarchy**'s **Entitlement Profiles**, to see Associated Roles for the access item.

How Roles are Created

IdentityIQ provides a comprehensive set of role engineering tools in the Role Management UI, to help your organization rapidly build and deploy an enterprise role model. These tools include an interactive role modeling interface as well as business and IT role mining capabilities.

Business roles and IT roles can be *manually* created through the Role Management user interface.

You can also use the *role mining* feature to generate business and IT roles; role mining can often do the task more efficiently than a manual process. Roles created through role mining can then be manually modified.

In business role mining, roles are identified based on one or more identity attributes in IdentityIQ. For example, if Job Title is one of the identity attributes, a business role can be created based on each unique Job Title.

In IT role mining, IT roles are generated based on system access current employees already have.

Both the Role Management UI and the Role Mining feature are discussed in detail later in this section.

How Roles are Assigned

Business roles can be assigned in a couple of ways. Roles can be assigned *automatically* based on attribute matching, using assignment rules in the business role. This is typically used for birthright provisioning – that is, simply because someone is an employee, they automatically get some set of business roles; furthermore, if they are in the Accounting department (as indicated by an attribute defining their department), they get another business role; and if they are also a manager, they may get yet another business role. This can all be done automatically when an identity is created, or when it is updated with, for example, a change of department or a change of manager status. Birthright roles are frequently marked as not requestable; they also could be excluded from the certification process, since we expect users to be granted these roles simply by virtue of who they are.

Roles can also be *requestable* – that is, a role can be assigned to a user based on a request for the role from, for example, the user's manager, an application manager, or from the user himself. Part of designing your role model includes determining who may request roles, and who will approve the role requests. When you define your roles, you can specify role attributes that determine what the approval process is.

Using Assignment Rules to Assign Business Roles to Identities

Automatic role assignment is done based on the **Assignment Rule** for the role. When roles are created through Role Mining, the Assignment Rule is automatically generated to match the selection criteria that created the role.

When the Assignment Rule is executed, the appropriate Identities are automatically assigned that business role. To execute the roles' assignment rules, run an **Identity Refresh** task with the **Refresh assigned, detected roles and promote additional entitlements** option selected. See the **Tasks** documentation for more information.

Manually created roles must have an Assignment Rule written for them to allow them to be assigned to Identities automatically. The assignment rule for each role can be defined through any of these constructs:

- **Match List**: checks for a match in one or more identity or application attribute values
- **Filter**: specifies matching criteria in a <CompoundFilter> XML representation.
- **Script / Rule**: BeanShell code that sets the criteria for assigning the role; usually used when the conditions for the assignment rule are too complex for the simpler constructs
- **Population**: saved set of search criteria identifying a population of identities; Populations are created from Advanced Analytics searches.

If role-mining-generated roles are manually modified, the assignment rules generated for them may no longer apply. In that case, the assignment rules must be edited as well to prevent them from being incorrectly assigned to Identities.

For an overview of developing and using rules in IdentityIQ, see the *IdentityIQ System Administration* guide.

Reviewing and Monitoring Roles and Role Assignments

Review of roles and role assignments is an essential part of successful roles program. Tools for monitoring role assignments include:

Manager and Targeted Certifications

These certifications allow managers to review roles assigned to their employees.

Role Membership Certifications

These certifications let the owner(s) of the role itself review all the users who have that role.

Role Composition Certifications

These certifications allow the role owner (or others) to review the access that makes up the role, to ensure that roles are accurate and current.

These options are discussed in detail in the IdentityIQ **Certifications and Access Reviews** documentation.

Role Based Access Control (RBAC)

Role-based access control (RBAC) is an approach to access security that relies on a person's role within an organization to determine what access they have. A role is a collection of permissions, and users receive permissions through the roles they have been assigned. Permissions or access in this definition can mean many things, such as the ability to perform certain tasks, permission to view, edit, or create files, or holding superuser privileges on sensitive applications, to give just a few examples. This allows roles within an organization to remain relatively stable while users and permissions can change rapidly.

One of the main goals of RBAC is to grant employees only the access they need to do their jobs, and to prevent them from having access that is not relevant to them. A well-designed RBAC system also simplifies and streamlines the

administration of access, by grouping sets of access in a logical and intuitive way, based on things like department, job function or title, region, or manager level. Grouping access permissions into roles provides a secure and efficient way of managing access, and helps keep things simple for administrators, certifiers, and the users requesting access.

Full versus Partial RBAC

RBAC is often talked about as a comprehensive system, but in actual practice it can be implemented as a partial solution. As you plan your organization's RBAC strategy, don't get too caught up in the idea that *all* access must be managed *only* through roles. A partial RBAC solution that manages some but not all access through roles can still provide a great deal of value. Trying to achieve 100% coverage for all access can easily result in a proliferation of roles, including the creation of roles which may have only one person in them. This can ultimately undercut the goal of making access easier and more efficient to manage.

Some job profiles are particularly well suited to an RBAC approach, such as jobs that involve a high degree of standardization, high turnover, seasonal employment, or a need for particularly rapid onboarding. Other job profiles, such as those in an IT department that involve highly privileged and specialized access, may not be good candidates for RBAC.

Implementing RBAC in IdentityIQ

IdentityIQ provides many features and tools that support implementation of RBAC: role editing and modeling, role mining, entitlement analysis, certifications for role membership and role composition, and workflows for governing changes.

Here are some key IdentityIQ concepts you should be familiar with as you plan your implementation of RBAC:

- IdentityIQ's Two-Tier Role Model
- Linking IT Roles to Business Roles: Required and Permitted Access
- How Roles are Assigned
- Reviewing and Monitoring Roles and Role Assignments

Maintaining Roles

An RBAC system is successful only to the extent that the roles it relies on are current, relevant, and appropriately scoped. In addition to monitoring who has a role, you have to monitor what is in a role. Within your organization, the types of available access can change, job descriptions can change, new applications can get added, et cetera. People in your organization must have confidence that roles are meaningful and current, or they may stop using them.

IdentityIQ offers some features to help you maintain your roles.

- The The Role Editor Page supports creating and editing roles. You can configure roles such that a change or edit to the role will trigger a workflow for approvals and notifications before the role is promoted into production.
- The Role Composition Certification allows the role owner (or others) to review the access that makes up the role. This certification is an essential part of a role program, for keeping roles accurate and current.See **How To Perform a Role Composition Access Review** in the *IdentityIQ Certifications and Access Reviews Guide*.

Best Practices for Defining and Creating Roles for RBAC

As you set about defining the roles for RBAC, you need a clear picture of the business roles in your organization, and of the entitlements. Part of this exercise is determining where to start implementing RBAC. It may not be realistic to try to set up RBAC for your entire organization all at once, and where you start will depend a lot on your type of business and your organization.

Here are some best practices for defining and creating roles:

- **Include business experts in the planning.** It's essential to work with your organization's subject matter experts – managers, IT and security teams, human resources, application owners, et cetera, who have a clear idea of what their team members do and how people use various applications – to help you determine which segments of your organization are most in need of RBAC. These business experts can also help identify patterns of access, define job responsibilities, and evaluate access options.
- **Monitor the big picture.** In addition to the business experts who will provide input on the needs of specific departments or applications, you also need someone with oversight over the entire role hierarchy to spot organization-wide patterns and see the big picture, in order to help you avoid role proliferation or duplication. There may be some overlap of access needs among disparate teams, so in order to avoid duplication of roles, you will need someone keeping track of the overall, top-level view of your role model.
- **Familiarize yourself with IdentityIQ's tools for role development.** IdentityIQ provides a number of tools to help with role creation: Entitlement Analysis , Role Mining for Business and IT Roles, and Role Modeling all support analysis of the data which has been onboarded into IdentityIQ, and can create roles based on that analysis. You can export role mining data and ad hoc queries into a report format for your analysts to evaluate.
- **Work with a meaningful entitlement catalog.** Before developing your roles in IdentityIQ, it helps to have a meaningful entitlement catalog from which to build roles. The Entitlement Analysis feature is one of the most useful ways of identifying patterns of access and spotting "red flags" or outliers with singular access assignments. The usefulness of the analysis depends on an entitlement catalog that completely and correctly represents the access you want to manage.
- **Use meaningful names and descriptions for business roles.** When you create business roles, keep in mind that it's important to use meaningful names and descriptions for the roles. These are available to people requesting and reviewing access and can be very valuable information to help users understand what each

business role is for, and what it includes.

- **Define your IdentityIQ team appropriately.** The people who analyze and define the roles and the access that goes with them do not have to be the same people who work in IdentityIQ to set roles up. Choose the right team of people for working on the role model in IdentityIQ so that your definition and implementation efforts are secure and efficient.
- **Create a process to approve role creation.** Plan for an approval process for role creation. Roles can be set up to trigger workflows for approval and notification. Putting new roles, or changes to roles, through an approval process protects against role proliferation/duplication.

RBAC Project Tips

Here are some pointers based on the experience of customers, partners, and SailPoint solution architects who have implemented RBAC in the field. While your own project requirements may vary and will depend on your business needs, these are things to consider as you plan your RBAC strategy:

- **Take a pragmatic approach.** Think of RBAC as an ongoing program, not a project. Don't expect to achieve 100% coverage of all access via RBAC as you implement it. A comprehensive RBAC solution could take months or even years to complete. It is realistic and acceptable to implement RBAC in steps or phases.
- **Know what you're trying to accomplish.** Are you trying to make certifications easier? If so, your primary focus will be on evaluating and organizing current access. Is your goal to make access requests easier? In that case, you may want to focus on the Lifecycle Manager side of IdentityIQ, using roles to help users more easily find and select the roles they want to request.
- **Look for groupings of role types.** Use the IdentityIQ features such as Role Mining and Entitlement Analysis to identify patterns and groupings of access and role types. This will help you avoid role proliferation.
- **Enforce least privilege.** Define roles so that you don't give people access they don't need. Setting up roles for the least privilege is a best practice for reducing security risk, both from malicious intent and from user errors.
- **Expect exceptions to RBAC.** In most enterprises, it is difficult or impossible to entirely avoid individual entitlements, especially in areas of highly specialized access needs, such as an IT department. Don't assume you have to force all entitlements and all access models into roles.
- **Make roles reusable.** If only one person in the whole organization has some particular role, maybe that access shouldn't be managed via a role. Make sure the roles you define are applicable to groups of people; otherwise your role model will be unwieldy and will not deliver the goals of efficiency and simplification.
- **Involve the business experts.** People within your organization who know the business are often the best resource for what the access patterns are and how should you structure your roles.

- **Test and verify your roles.** Roles need as much testing and verification as other functionality – maybe more. If you define roles sub-optimally at the outset and put them into production, you can end up with a lot of users who lack the access they need or who have more access than they should. There can be a big cleanup effort if you roll out a role structure that has not been set up and tested properly.
- **Develop processes for role maintenance.** Roles evolve, and you need to keep them up to date. Plan for periodic review and certification of your roles to make sure they're still current and accurate. You should also plan for how to retire roles when they are no longer needed. Regular certification of role composition and role membership should be part of your ongoing RBAC strategy.

Global Configuration and Settings for Roles

System administrators can set global configurations and global defaults for roles and role behavior. These functions are available through the administrator "gear" menu in IdentityIQ. For more information, see the **System Configuration** documentation. Here is a brief overview of the administrator options for roles, and where to find them in the administrator UIs:

gear > Global Settings > IdentityIQ Configuration > Roles tab

On this tab you can enable the use of, and default settings for, sunrise and sunset dates for roles. Sunrise and sunset dates let you make roles and entitlements temporary, to control when a role (or an individual user's access to a role or an entitlement) becomes active, and when it becomes inactive. If you want to use sunrise and sunset dates for roles, you must enable the feature globally here before setting sunrise and sunset dates on specific roles in the Role Management UI.

gear > Global Settings > Role Configuration

Use the Edit Role Configuration page to define custom extended role attributes and role types. The extended attributes are displayed with the rest of the role information throughout IdentityIQ. An example of a extended role attribute might be role status. 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.

gear > Global Settings > Forms

Here, you can create forms for gathering user input at the time a role is requested.

gear > Lifecycle Manager Configuration > Configure tab

On this tab, you can select the role types that are available for role requests.

Role Modeling

To access the Role Management page, click **Setup > Roles**.

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.

Terms used in role modeling:

Role Mining

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. See Role Mining for more information.

Business Role Mining

Within IdentityIQ, business role mining 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. See Business Role Mining for more information.

Entitlement Analysis

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. See Entitlement Analysis for more information.

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

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

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

Role activation events enable you to use business processes to automatically activate or deactivate roles based on dates you configure for the role. Role activation business processes can be configured to automatically refresh identities to include or exclude the impacted roles.

IdentityIQ user rights

Granting 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 Viewer Tab

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

The **Role Viewer** tab of the Role Manager lists your existing roles, displays detailed information about each role, and lets you add, edit, and delete roles. The Role Viewer tab lets you work with these IdentityIQ components:

- Roles — See The Role Editor Page
- Archived Roles — See Role Editor - Archived Role Panel
- Profiles — See Role Editor - Edit Entitlement Panel

Viewing Role Information

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.

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.

Role Information Panel:

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. 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.

Classification

Classifications categorize and flag a role, to identify it as potentially allowing access to sensitive, privileged, or otherwise significant data.

Elevated Access

This will be set to true or false depending on if the role has elevated access.

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.

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.

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.

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. These capabilities and scopes are not assigned until a Identity Cube Refresh task is run with the Provision assigned roles option selected.

Adding Roles from the Role Viewer

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. For more information on adding roles, see How to Create or Edit a Role From the Role Management Page.

Deleting Roles in the Role Viewer

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

The 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.

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

> 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 roletype”.

Roles that are awaiting approval are displayed with a red square around the role icon. You can 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.

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.

Role Editor Fields

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. 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.

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.

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

Enables a role to be assigned to the same identity multiple times. This option is not available if either multiple assignments are not enabled, or if they are universally enabled. 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 are displayed with the role information. You can enter data in any of these attribute fields, to be used in rules and workflows written for your installation.

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.

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.

These capabilities and scopes are not assigned until an Identity Refresh task is run with the Provision assigned roles option selected. See the **Tasks** documentation for more details.

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 may 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 for information on how to work with profiles.

Simple View Fields on the Entitlement Editor panel:

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.

Advanced View Fields on the Entitlement Editor panel:

Description

A brief description of the profile.

This description is displayed with the role throughout the product and should be as intuitive as possible.

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.

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

The value of the attribute. When available, select an entitlement from the drop-down list. This field is not available for unary operations.

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 for information on how to work with provisioning policies.

The Provisioning Policy Editor panel contains the following information:

Edit Provisioning Policy Fields

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.

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 The Role Editor Page 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.

The 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 Role Index Refresh task must have run at least once before a roles search can yield results. See the **IdentityIQ Tasks** documentation.

The search fields are "AND" type searches. Only actions matching values specified in *all* fields are included in the search results.

If you do not enter any values in a search criteria field, all possible choices are included for that field. For example, if you do not provide a type in the **Type** field, roles of any type are included.

Specify the search criteria and columns to display and click **Run Search** to display the search results. From the search results page you can review the results of your search and save the search.

Role Attributes

Name

Enter a role name to include in the search.

Entering a string of characters returns all roles with that string in their name that your controlled scopes enable you to view. For example, if you enter *admin* the search results include information for the roles System Administrator, SysAdmin, and Administrative Assistant.

Display Name

Enter a display name to include in the search.

Entering a string of characters returns all roles with that string in their display name that your controlled scopes enable you to view. For example, if you enter *System Administrator* the search results include information for the display name System Administrator.

Owner

Enter the role owner to include in the search.

Click the arrow to the right of the suggestion field to display a list of all role owners, or enter a few letters in the field to display a list of role owners that start with that letter string.

Type

Select the role type to include in your search. For example, IT, Organizational, or Business.

Role types are defined for your enterprise during the role modeling process.

Status

Select the Enabled/Disabled status of the roles to include in the search.

Classification

Classifications can identify roles as potentially allowing access to sensitive, protected, or otherwise significant data. Choose any classifications to include in the search.

Detected Total

Specify an upper or lower limit for the number of identities that have this role detected that should be included in the search results.

Detected roles are roles that are automatically assigned to identities based on the entitlements to which they have access.

For example, to search for roles that were not detected by any identity during correlation, select Less Than from the drop-down list and type **1** in the empty field. The search results include all roles that were not automatically assigned to at least one identity.

Assigned Total

Specify an upper or lower limit for the number of identities that have this role assigned that should be included in the search results.

Assigned roles are roles that were manually assigned to an identity by a user with role assignment authority or through a role assignment rule.

For example, to search for roles that were not assigned to any identity, select Less Than from the drop-down list and type **1** in the empty field. The search results include all roles that were not manually assigned to at least one identity.

Entitlement Total

Specify an upper or lower limit for the number of entitlement a role can have.

For example, if you select Less Than and type **3**, the search results include roles that contain two (2), one (1), or zero (0) entitlements.

Risk Score Weight

Specify an upper or lower limit for risk score weight assigned to a role for it to be included in the search results.

For example, you can specify a Greater Than value to search for high-risk roles, or you can specify a Less Than value to search for roles that were created with a risk score weight that is too low for their type. In the second example, if your enterprise has a policy that requires that all IT-type roles have a risk score weight of 100, you can select IT from the **Type** drop-down list, select Less Than from the **Risk Score Weight** drop-down list, and type 100 in the empty field to return all IT-type roles with a risk score weight less than 100.

Associated To Another Role

Include roles that are associated with at least one other role or roles that are NOT associated with any other role.

True — include roles that are associated with at least one other role.
False — include roles that are NOT associated with any other roles.

Effective Access

Limit the search to the specific effective access list.

Effective Access is any indirect access that was granted through another object. For example a nested group, an unstructured target, or another role.

Filter by: Profile

A profile is a set of entitlements on a specific application. Options in this section let you search for roles based on profiles and on their relationship to other roles.

Profile State

Search for roles based on how entitlements and permissions are defined relative to the role(s). For example, you can use this criteria to search for all roles on an invalid application, or for roles with entitlements that are not defined (in other words, are missing) in IdentityIQ.

Options are:

- No Invalid/Missing Relationships
- Invalid Applications or Missing Entitlements/Permissions
- Missing Entitlements/Permissions Only
- Invalid Applications Only

Relationship to Role

Search for roles based on how entitlements or permissions are defined, relative to the role(s). This filter can be used in conjunction with an application, or independently. For example, to search for roles that provide direct access to permissions on the Oasis_DB application, you would select the **Oasis_DB application**, select **Permissions** in the **Filter Type** field, and choose **Any direct relationships** here. To search for every role that allows indirect access to entitlements, regardless of the application, you would select **Any indirect relationships** here and choose **Entitlements** in the **Filter Type** field.

Options are:

- Any direct or indirect relationships: Show roles with any entitlement or permission relationships
- Any direct relationships: Only show roles that have the entitlements or permissions directly on them
- Any direct and selected indirection relationships: Show roles that have the entitlements/permissions directly on them, or a specific indirect relationship (such as inherited, permitted, or required). When you choose this option, you can enter additional criteria to filter on **Inheritance** and **Required/Permitted** relationships.
- Any indirect relationships: Only show roles that have entitlements or permissions through a specific relationship, not on the role directly

- Selected indirect relationships: Only show roles that have the entitlement or permission through a specific relationship, not on the role itself. When you choose this option, you can enter additional criteria to filter on **Inheritance** and **Required/Permitted** relationships.

Note that some roles can grant both direct and indirect access to entitlements and permissions, so a role can potentially be returned by both the direct relationship and indirect relationship options.

Application

To filter roles by application, choose the application(s) here.

Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.

Filter Type

Choose whether to search for permissions or entitlements. Leave this field blank to search for both.

Filter by: Extended Attributes

The extended attributes for roles are specific to your instance of IdentityIQ; they are defined under the **gear icon > Global Settings > Role Configuration** option. Any extended attributes defined for roles that are marked *searchable* appear here as search critiera.

Filter By: Date

Date Type

Select a state to associate with the specified dates:

Last Membership Certification — the date when the last role membership certification was performed.
Last Composition Certification — the date when the last role composition certification was performed.
Last Assigned — the date when the role was last assigned to an identity.

Start Date

Specify a beginning date for this search. The search results include information pertaining to any action performed on or after the specified date.

End Date

Specify an end date for this search. The search results include information pertaining to any action performed on or before the specified date.

Fields to Display

Choose the information to display on the Role Search Results page associated with this search. Each field defines a column on the results table.

You must select at least one field to display on the results page.

Saving Searches

Once you have run your search, you can save the results as a saved search or as a report.

1. In the **Search Results** page, click the **Result Options** drop-down and choose **Save Search** or **Save Search as Report**.
2. Enter a **Name** and **Description** for the saved search or report.
3. Click **Save**.

Searches saved as *reports* are saved in the **Intelligence > Reports > My Reports** area of IdentityIQ. Searches saved as *searches* are listed in the **Saved Searches** section of the Role Search page.

When you have saved searches, you can:

- Click on the saved search in the **Search Name** area, to see the saved search's description and to load the criteria for the search.
- Clear any saved search criteria you have loaded by clicking the **Clear Search** button at the bottom of the page.
- Delete the currently-selected saved search by clicking **Delete Search**.

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 for more information.

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 for more information.

To Create a Role

1. To 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** — The name of this role; this serves as the programmatic name for the role in the IdentityIQ object model. Single quotation marks, double quotation marks, or commas are not supported in the Name.
    - **Display Name** — A user-friendly descriptive name of this role. The Display Name is used throughout IdentityIQ, in access requests, approvals, and certifications.
    - **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. **Enable Activity Monitoring** Select this if you want to track activity for any user who is assigned this role.
5. **Provision both profiles and policies** If a provisioning policy has been defined on a role, it supersedes the entitlement profile in provisioning operations. This flag indicates that you want it to supplement the entitlement definition instead of override. Provisioning policies and entitlement profiles can be defined for this role in later steps.
6. **Disabled**. Select this option to disable the role. Disabled roles can not be assigned or used to manage access.
7. **Custom or Extended Role Attributes:** Any extended role attributes configured for your enterprise are displayed with the role information. You can enter data in any of these attribute fields, to be used in rules and workflows written for your installation.
8. Perform any optional tasks necessary to create or edit the role. See Optional Tasks , below.
9. For IT roles, add the entitlements to the role (or edit or delete existing entitlements) from the **Entitlements** panel. Entitlement profiles created for this role are inherited by any role that is a member of this role.
10. When you have finished creating a new role or editing an existing role, 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.

Optional Tasks

The following tasks can be performed when you create a Role. You can choose to do some of them or all of them prior to saving the role.

Define Classifications for the role

Classifications can categorize and flag a role, to identify it as potentially allowing access to sensitive, privileged, or otherwise significant data. Choose any classifications you want to add to this role from the the drop-down list. The list includes any classifications that have been configured in your system; if no classifications have been defined, the list is empty. See the **Classifications** documentation for more information.

Define Scheduled Activation and Deactivation Events for the role:

Scheduled events use business processes to automatically activate or deactivate roles based on the dates set in the **Add New Event** dialog within this section. This section will appear only if your instance of IdentityIQ has been configured to allow for sunrise and sunset dates for roles. See the **System Configuration** documentation more information on enabling sunrise and sunset dates.

> Note: Only one activation or deactivation event can be defined at a time.

1. Click **Add Event** to display the **Add New Event** dialog.
2. Manually enter a date or click the calendar icon to select a date.
3. Select **Activate** or **Deactivate** from the **Action** drop-down list.
4. Click **Save** to return to the Role Editor page.
5. Select an event and click **Delete** to remove the event.

Define an Assignment Rule

Assignment rules are used in Business roles to define logic allowing them to be assigned to Identities automatically. An Assignment Rule can be defined using these options:

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.

Modify the list of roles permitted by this role

Click **Modify Permitted Roles** in the Permitted Roles panel and modify the list of roles permitted by this role.

1. Enter the first few letters of a role name in the **Select a role** field and select a role from the selection list.
2. Click **Add** to add the role to the membership list.
   Add as many roles as required.
3. Click **Save**.

Modify the list of roles required for this role

Click **Modify Required Roles** in the Required Roles panel and modify the list of roles required by this role.

1. Enter the first few letters of a role name in the **Select a role** field and select a role from the selection list.
2. Click **Add** to add the role to the membership list.
   Add as many roles as required.
3. Click **Save**.

Modify the list of roles which this role is a member

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.

1. Enter the first few letters of a role name in the **Select a role** field and select a role from the selection list.
2. Click **Add** to add the role to the inheritance list.
   Add as many roles as required.
3. Click **Save**.

> Note: Any roles that have elevated access will display with an icon next to the name of the role.

Add a Provisioning Policy for this role.

Provisioning policies define the fields required for a role to be provisioned, often including a default value or script/rule for calculating a value. The policies available to be assigned to the rule are listed in the Provisioning Policy panel. Click **Add Provisioning Policy** to create a new policy, or **Delete Provisioning Policy** to remove any existing policies.

See the Role Editor - Provisioning Policy Editor Panel and the **Provisioning** documentatoin or more information.

Additional Information

To work with profiles associated with a role see:

- How to Create or Edit a Profile
- How to Create a Profile Using Entitlement Analysis

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.

Create a new role from a role creation request

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 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.

To approve role changes:

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 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.

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. For information about creating a profile using entitlement analysis, see How to Create a Profile Using Entitlement Analysis.

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

Create a New Profile from the Simple View

> 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.

Create a New Profile from the Advanced View

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 Profile.
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 How to Create or Edit a Profile. For an explanation of the permission options, see How to Create or Edit a Profile.
6. Click **Save** to return to the Role Editor.

Edit a profile

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

Additional Information

From the Role Editor you can add additional profiles, edit the role, or save the role. See The Role Editor Page.

Profile Attributes

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 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 foraccess 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.

Overview

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

- Search for entitlements
- Analyze the search results
- Save the profile

Search for Entitlements:

1. Access the Create Profile from Entitlement Analysis panel.
2. 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 Profile.
3. Select the application on which to search for entitlements.
4. *Optional:* Narrow your entitlement search using the Identity Attribute fields.
   The Identity Attribute fields displayed are dependent on the identity attributes defined during configuration.
5. 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.

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 The Role Editor Page.

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.

> 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.

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

To perform impact analysis

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.

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.

Column	Description
Search Parameters:	
Attribute	The criteria used to define this search. For example,

Column	Description
	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.

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
- Business Role Mining

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.

Types of Role Mining Activities

Roles can be mined either by performing a Role Mining process or by running an Entitlement Analysis . Both options are found on the Role Management page. These two options are similar in some ways:

- Both allow the administrator to specify one or more applications whose entitlements will be evaluated as well as a set of identity attributes that can be used to filter the set of Identities that should be examined.
- Both only return entitlements held by at least one identity in the examined set. This is useful for constraining the role modeling activities to manageable sets by looking at users who are likely to share common sets of entitlements that should be configured as IT roles (e.g. users in the Accounting department or the Austin location).

They each also offer unique features in role creation that make them separately suited to different types of role creation needs.

IT Role Mining is designed to highlight Identities' entitlement commonalities. It returns every set of entitlements on the selected applications that are all held by one or more Identities. It does not return subsets (e.g. if several identities hold entitlements A, B, and C but none hold A and B without C, ABC will be a returned set but AB will not be a returned set of its own).

Entitlement Analysis is designed to allow maximum flexibility in grouping entitlements into roles by returning each entitlement separately and allowing the administrator to group them in as many combinations as are desired. Entitlement Analysis even allows the creation of roles that represent sets of entitlements no one user currently holds, while IT Role Mining does not. (Using the example scenario above, entitlement analysis supports the creation of a role containing entitlements A and B only while IT Role Mining does not.) However, Entitlement Analysis does not show the existing connections between entitlements as well as IT Role Mining does. See Entitlement Analysis .

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.

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

> Note: The role mining task fails if the number of candidate roles discovered exceeds the number specified in this field.

Specify the maximum number of groups (candidate roles), which can be generated using this role mining criteria.

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

> 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.

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.

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.

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

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

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

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

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.

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 for all newly-generated roles based on the scoping attribute. If selected, a dropdown appears for the type of root container role to generate. For example, if roles are mined based on the Department attribute and you specify the type of root container as Organizational, then an Organizational container is created for each of the Department roles that are mined.

Use this option when you want to organize roles into separate containers based on the scoping attribute, rather than using one container for all generated roles.

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

> This option is hidden when the **Perform Analysis Only** is selected on the business role mining page.

Type of role generated by the task.

Owner

> Note: This option is hidden when the **Perform Analysis Only** is selected on the business role mining page.

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.

Minimum Number of Users per Role

Minimum number of users who must meet the mining criteria before a role is generated.

Naming Algorithm

> Note: This option is hidden when the **Perform Analysis Only** is selected on the business role mining page.

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.

Prefix to Apply to Generated Role Names

> Note: This option is hidden when the **Perform Analysis Only** is selected on the business role mining page.

Prefix to add to the generated role names.

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

> 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.

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.

Organizational Roles as Container Roles in Role Mining

Roles created through business and IT role mining activities are automatically generated in "container" organizational roles by the mining operations. Container roles are a useful way to organize these system-generated roles, either temporarily before they are reassigned to organizational units representing a different structure or permanently as a place where the generated roles can be tracked and maintained by an administrator. IT roles are frequently left in these container organizational roles, even if mined business roles are moved to a different structure.

The placements of roles in organizational roles do not affect IdentityIQ’s usage of them; the structure just needs to be clear to the administrators who will navigate through it to manage the roles.

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.

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
- Business Role Mining Results Details

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.

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

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.
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.

Using Sunrise and Sunset Dates for Temporary Access

"Sunrise" and "sunset" dates are used to make roles and entitlements temporary - they determine when a role (or an individual user's access to a role or an entitlement) becomes active, and when it becomes inactive.

This feature offers an efficient, automated way to grant time-limited access to sensitive roles, roles that are seasonal or temporary, or access that for any reason is intended to have a limited duration, such as a short-term assignment to a different team or a special project.

IdentityIQ gives you two ways to use sunrise and sunset dates:

- On roles themselves, so that the role itself has a temporary duration.
- When a role or entitlement is granted to a specific user; in other words, the role itself may not have time limits, but a certain user's access to that role should have a limited duration.

Using Sunrise and Sunset Dates for User Access

Even if a role itself does not need to be limited to a temporary duration, you may want to grant some users only temporary access to certain roles or entitlements. Note that while the sunrise and sunset dates for roles as described above apply to roles only, the sunrise and sunset dates you can set for individual users can apply to both roles and entitlements.

Enabling the Feature

To enable sunrise/sunset dates for individual user access:

1. Click **gear menu > Global Settings > IdentityIQ Configuration**
2. On the **Roles** tab:
    - In the **Role Sunrise/Sunset Dates** section, check the option to **Enable Sunrise/Sunset Dates on Role Assignment**
    - In the **Business Processes** section, select a business process for managing activation/deactivation in the **Scheduled role/entitlement assignment** drop down. A standard business process ("Scheduled Assignment") is provided out of the box, but you can implement a custom business process if your business needs require one.
3. **Save** your changes.

Using Sunrise and Sunset Dates in Access Requests

Once sunrise and sunset dates are enabled for role assignment, the access request UI will include a calendar widget for setting the start and end dates for the access. This widget is on the **Review and Submit** tab.

If your access request includes more than one item, you can set a single date range for the entire request, or individual date ranges for each role or entitlement in the request.

Click the calendar widget to set the dates for access.

You can also use the comments widget to add information about the request and why it is temporary. Be sure to **Save** your information.

For more information, see the **Lifecycle Manager** documentation.

Using Sunrise and Sunset Dates in Access Approvals

Users responsible for approving a request for access can see any sunrise/sunset dates in a request item, and can change the dates as part of the approval process.

The calendar widget is green in any request item that includes sunrise and sunset dates, to alert the reviewer that there is a date range specified for the access.

The reviewer can click the calendar widget to see the sunrise and sunset dates. The reviewer can also modify the dates as needed in this dialog.

Extending Sunset Dates for Users

Once an access request with sunrise and sunset dates has been approved, the sunrise date can not be modified. However, the sunset date can be extended through a request to remove access.

To request an extension to the sunset date:

1. From the Quicklink menu, select **Manage User Access** (for managers) or **Manage My Access** (for the individual user in question) to open the Manage Access UI.
2. If required, select the user, and click **Next**
3. On the **Manage Access** tab, click the option to **Remove Access**.
4. Find the role to be extended and click the x icon to select it.
5. Click **Next**.
6. On the **Review and Submit** tab, click the calendar icon.
7. Choose the new Sunset date and click **Save**.
8. **Submit** the request.

The request to extend the sunset date follows the same approval path as a request for access.

Viewing Temporary Access for Users

You can see when a user's access is temporary from the **Manage Identity** Quicklink menu, under **View Identity** or **Edit Identity**, in the Access page.

You can also see which access is temporary in **Identities > Identity Warehouse**, on the **Entitlements** tab for the user:

Using Sunrise and Sunset Dates for User Access

Even if a role itself does not need to be limited to a temporary duration, you may want to grant some users only temporary access to certain roles or entitlements. Note that while the sunrise and sunset dates for roles as described above apply to roles only, the sunrise and sunset dates you can set for individual users can apply to both roles and entitlements.

Enabling the Feature

To enable sunrise/sunset dates for individual user access:

1. Click **gear menu > Global Settings > IdentityIQ Configuration**
2. On the **Roles** tab:

- In the **Role Sunrise/Sunset Dates** section, check the option to **Enable Sunrise/Sunset Dates on Role Assignment**
- In the **Business Processes** section, select a business process for managing activation/deactivation in the **Scheduled role/entitlement assignment** drop down. A standard business process ("Scheduled Assignment") is provided out of the box, but you can implement a custom business process if your business needs require one.

3. **Save** your changes.

Using Sunrise and Sunset Dates in Access Requests

Once sunrise and sunset dates are enabled for role assignment, the access request UI will include a calendar widget for setting the start and end dates for the access. This widget is on the **Review and Submit** tab.

If your access request includes more than one item, you can set a single date range for the entire request, or individual date ranges for each role or entitlement in the request.

Click the calendar widget to set the dates for access.

You can also use the comments widget to add information about the request and why it is temporary. Be sure to **Save** your information.

For more information, see the **Lifecycle Manager** documentation.

Using Sunrise and Sunset Dates in Access Approvals

Users responsible for approving a request for access can see any sunrise/sunset dates in a request item, and can change the dates as part of the approval process.

The calendar widget is green in any request item that includes sunrise and sunset dates, to alert the reviewer that there is a date range specified for the access.

The reviewer can click the calendar widget to see the sunrise and sunset dates. The reviewer can also modify the dates as needed in this dialog.

Extending Sunset Dates for Users

Once an access request with sunrise and sunset dates has been approved, the sunrise date can not be modified. However, the sunset date can be extended through a request to remove access.

To request an extension to the sunset date:

1. From the Quicklink menu, select **Manage User Access** (for managers) or **Manage My Access** (for the individual user in question) to open the Manage Access UI.
2. If required, select the user, and click **Next**

3. On the **Manage Access** tab, click the option to **Remove Access**.
4. Find the role to be extended and click the x icon to select it.
5. Click **Next**.
6. On the **Review and Submit** tab, click the calendar icon.
7. Choose the new Sunset date and click **Save**.
8. **Submit** the request.

The request to extend the sunset date follows the same approval path as a request for access.

Viewing Temporary Access for Users

You can see when a user's access is temporary from the **Manage Identity** Quicklink menu, under **View Identity** or **Edit Identity**, in the Access page.

You can also see which access is temporary in **Identities > Identity Warehouse**, on the **Entitlements** tab for the user:

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

Roles are detected when an **Identity Refresh** task runs with the **Refresh assigned, detected roles and promote additional entitlements** option is selected.

In role detection, IdentityIQ compares the entitlement profiles of each role to the entitlements held by each Identity. Profiles may specify a single entitlement or may specify multiple entitlements, either in “and” relationships, requiring the identity to have all listed entitlements to have the role, or “or” relationships, meaning the identity has the role if they have any of the entitlements. When an Identity’s collection of entitlements meets an IT role profile’s requirements, the role is marked as “detected” for that Identity.

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, if it was 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.

Defined IT roles can be detected for Identities based on the entitlements recorded for the Identity in IdentityIQ. Once entitlements are associated as a role for an Identity, the individual entitlements are no longer displayed on the Identity Cube's entitlements page, as they are replaced by the more concise role name. For example, if an Identity already has the time-tracking system's required entitlements for the Timesheet Approval role, this role will be detected for the Identity and will be marked on the Identity Cube in place of the entitlements encapsulated within it. The role-encapsulated entitlements can be shown or hidden in the UI based on a checkbox selection, and any role can be clicked to view the details within it.

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.

Propagating Role Changes

The **Propagate Role Changes** task manages updates to identities' entitlements when changes occur in the role model. Specifically, this task is necessary to manage removal of entitlements which are removed from role definitions, although it will propagate additions to role definitions as well.

Follow these steps to configure and use this task:

1. Click **gear > Global Settings > IdentityIQ Configuration** and click the **Roles** tab. Select **Allow propagation of role changes**. This turns on the creation of RoleChangeEvents, which record changes to the composition of any role. Be sure to **save** your changes.
2. Navigate to **Setup > Tasks** and choose **New Task > Propagate Role Changes**. This task can be configured to run policy checking as it updates identities' role and entitlement data to match the role changes. It can also be configured to run for limited time durations; when a number of minutes is specified, it will not start processing a new event when that number of minutes is reached, but it will process the current event to completion before terminating, even if that extends past the time limit.
3. **Schedule** the task to run on a regular basis, as appropriate for the installation's role model change volumes and role management preferences. Role changes are captured and propagated for the role on which the change occurred and for any role which inherits from or requires the changed role.

For more information see the **Tasks** documentation.

Automated Propagation of Role Changes to Role Members

The role propagation feature in IdentityIQ allows any changes made to a role, including new and removed roles, changes in hierarchy, and changes in entitlements, to be propagated to all identities that are assigned that role. This

allows you to use the role model as an authoritative source for requested access.

> Note: Entitlements that were detected are not removed from an identity during role propagation, unless they are also part of an assignment.. Only those entitlements that were assigned, individually or as part of a role assignment, are removed during propagation.

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

Globally Enabling Role Propagation

To use role propagation, the feature must be enabled globally. This is done in the **gear menu > Global Settings > Configuration > Roles** tab.

To enable role propagation, select the **Allow propagation of role changes** option on the Roles tab.

How Roles Are Propagated

Once role propagation is enabled, role changes can be automatically provisioned when the role propagation task is run. Changes are provisioned to all identities that are assigned the role that is being propagated.

When a role is changed, the change is saved as a **RoleChangeEvent**. The Propagate Role Changes task processes these events, provisioning the role changes to the identities that have that role assigned directly or indirectly.

Changes are saved and provisioned in the order they were created; in other words, in a "first in, first out" sequence. Consider this example of role changes, made in this sequence:

1. Add entitlement A
2. Remove entitlement A

In this example, the end result is that the identities with this role should not have entitlement A. If the sequence were reversed, the end result would be that the identities would have entitlement A. Understanding the sequential nature of role changes is important for error handling and troubleshooting.

The provisioning plan for all role change events is calculated before the task starts, when the role change occurs, and only role change events created before the Role Propagation task runs are processed by the task during that run. This means that changes to roles that are made after a role propagation task has begun will not be included in that run of the task.

To learn more, see the **Task** documentation.

Troubleshooting and Managing Errors in Role Propagation

There are several ways you can manage errors and troubleshoot role propagation activity.

Duration limits

A role propagation task can be configured with a "Number of minutes task should run" setting, which is the maximum number of minutes the task should run before terminating. After each event is processed, IdentityIQcompares the actual task duration to the specified maximum; if the task has run out of time, the task is terminated without proceeding to the next event. Note that the duration is not checked in the middle of an event, so an event will not be cut off without having a chance to finish.

Retrying failed identities

When an error occurs that causes an identity to failing on a given role change event, IdentityIQ does not delete the role change event. It keeps track of any identity that failed for the event, and on a second run of the task, can process the role change event only for those identities that failed in an earlier run.

Pruning “stuck” events

If a failure occurs that can’t be resolved with a retry, the role change event can potentially stay “stuck” in the processing queue indefinitely. The Role Change Propagation Task includes a parameter that allow the pruning of stuck events: **Maximum failures before event pruning**. This parameter sets the number of times a role change event can fail to progress before it is pruned. A failure to progress is defined as zero successes on the event during the task. Events that are blocked by other pending events are not counted as failing to progress. If this value is left blank, the event will never be pruned until it has been fully processed.

Setting a task failure threshold

The task also includes a **Maximum failure threshold** parameter that limits how many identities can fail to be provisioned by a single role change event, expressed as a percentage of the total number of identities affected by the event. All partitions for a role change event are allowed to run to completion, and once finished, the transition request computes the actual failure percentage and compares it to the maximum failure threshold. If the percentage is exceeded, the propagation terminates. Note that this does not mean that a single role change event will stop as soon as it hits the maximum; it means that if an event exceeds the maximum, no more *subsequent* events will be processed.

Evaluating results

Once the task has run, the Task Result UI shows various statistics, including errors. For role propagation, the **Number of identities failed/pending** and **Number of stale events pruned** statistics can be useful in troubleshooting errors. In the Debug pages, the **TaskResult** and **RoleChangeEvent** objects can also be

reviewed for troubleshooting purposes.

Role Changes on Disconnected Systems

By default, neither the Identity Refresh task nor the Role Propagation task will push entitlement changes to target systems when a manual work item is required to support provisioning. To do so could result in an overwhelming number of manual work items from even a single role definition change.

With the Identity Refresh task, there is a task option that allows you to request generation of manual work items for provisioning requests. It is called **Enable the generation of work items for unmanaged parts of the provisioning plan**.

This option does not exist in the Role Propagation task. Instead, in the Role Propagation task, there is an option to have the task run a business process in which you can do whatever you choose (including forcing the creation of manual work items). That business process must be named in the `systemConfiguration` Configuration object, in an entry called `workflowLCMRolePropagation`.

Keep in mind that provisioning of these un-propagated changes can also be handled on a user-by-user basis, as they will be visible in certifications. Un-propagated role content additions will appear as "missing required roles" in a certification, and un-propagated role content removals will result in the "extra" entitlements or IT roles appearing individually in the certification details. The certification can then trigger manual provisioning work items to process additions, or an informed certifier could revoke the no-longer-required extra access.

Role Change Propagation on Import

If you need to import role changes or new role definitions without creating role change events and initiationg role propagation, you can set an option on the import to suppress role change event creation. In the iiq console this option is `-noroleevents`.

For example, to import roles specified in a file called roles.xml without creating role events for role propagation, specify this command in the iiq console:

```
import -noroleevents roles.xml
```

In the **Import from File** page (**gear menu > Global Settings > Import from File**), you can suppress role change event creation by selecting the **option No role events generated for role propagation**.

For more information see the **IdentityIQ Console** and **System Configuration** documentation.

Certifying Roles

Simplifying the certification process is a key benefit of implementing roles. Both assigned business roles and detected IT roles are shown on certifications. Detected roles only show as independent line items in a certification if they are not required or permitted by an assigned business role for the identity; when they are part of an assigned business role,

they are hidden behind the business role in the certification process, though they can be seen by drilling into the business role details

When certifiers revoke a business role, they are prompted to choose which of the required and permitted IT roles to revoke as well. The underlying entitlements are only revoked when the required/permitted IT roles which include them are revoked.

For more information on how to certify roles, see the **Certifications and Access Reviews** documentation.

Versioning Roles

IdentityIQ supports saving and restoring of old versions of roles so changes can be rolled back when needed. Logic to support this functionality is present in both of the role modeler business processes provided out of the box: **Role Modeler - Owner Approval** and **Role Modeler - Impact Analysis**. By default, this functionality is turned off, but it can easily be activated.

When role changes occur, a business process is launched to process the changes; this may perform approval processes, impact analyses, and more. The business process that is launched is configured as part of the IdentityIQ configuration. The configuration setting is under the **gear menu > Global Settings > IdentityIQ Configuration > Roles** page as the **Role create, update, and delete business process**.

To enable versioning of roles, this business process must have the `doArchive` variable set to `true`. This is done through the Business Process Editor (**Setup > Business Process** > select business process) or through the business process XML.

Any time a role is changed (after any approval processes have finished and the change has been fully activated), an archive version of its previous state is saved. To view the set of previous states for a role, click the role name in the Role Viewer Navigation list (**Setup > Roles > Role Viewer** tab). In the **Role Information** pane to the right, locate the **Archived Roles** header and click the down arrows to view the list.

Click any version in the list to see its details and click **Roll Back to Archived Role** to open the archived version in the Role Editor. Then scroll down and click **Submit** to restore the archived version as the active version of the role. The version being replaced is then also created as another archived version.

The same rollback option is also available from the **Role Editor** page (visible by clicking **Edit Role** from the **Role Viewer** page). Find the **Archived Roles** section, expand it to view the archived versions, and click one to see its details. To restore that version, click **Roll Back to Archived Role**, and **Submit**.

Identities which are connected to a role, through assignment or detection, prior to the archive rollback retain their association to that role until a new **Identity Refresh** task is run with the **Refresh assigned, detected roles and promote additional entitlements** option selected. This will update those associations unless the role change business process itself is configured to do a refresh. If the role profile or assignment rule changed as part of the rollback, the role's new state may cause the role to be removed from some Identities and added to others as a result of the refresh process.

For more information on configuring global settings for Roles, see **the System Configuration** documentation.

For more information on working with business processes, see **the Business Processes** documentation.

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
- Managing IdentityIQ Access
- Creating Workgroups

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 responsibilities 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.

Managing IdentityIQ Access

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.

Creating Workgroups

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.

Populations and Groups

Populations and Groups are used to 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

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, or 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

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

Populations are created by setting up query criteria in the **Advanced Analytics** page of IdentityIQ and saving the results of the query as a population. To access the Advanced Analytics page, click **Intelligence > Advanced Analytics**.

You can create populations from two types of search in Advanced Analytics: the basic **Identity Search**, and **Advanced Search**. Identity Search allows you to set simple filter values for Identity Attributes to define the population. With Advanced Search, you can specify more complex search criteria, including grouping the filter criteria, choosing “and” or “or” relationships between criteria, and specifying search types other than “equals”.

For more information, see the **Search** documentation.

Basic Identity Search

The default Advanced Analytics search option is Identity Search, which offers a variety of Identity Attributes 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 option is accessed by clicking **Advanced Search** on the Identity Search tab. This option gives you more flexibility in setting your 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.

You can edit the filter source directly by clicking [**view /edit filter source**]. This gives you even more flexibility in setting filter criteria in ways that might not be available through the user interface.

For more detailed information on working with filters and filter strings, see the Filters and Filter Strings technical white paper on Compass.

If filters are modified and saved using the filter source , 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(Iden-
tityExternalAttribute.objectId) && IdentityExternalAttribute.attributeName i== \"Iden-
tityAttributeName\" && IdentityExternalAttribute.value.startsWith
(\"attributevalue\")))")
```

or

```
LinkExternalAttribute.collectionCondition("((links.id.join(LinkEx-
ternalAttribute.objectId) && LinkExternalAttribute.attributeName i== \"Ac-
countAttributeName\" && LinkExternalAttribute.value.startsWith
(\"attributevalue\")))")
```

The table below details the syntax for adding filters of various data types to the filter source.

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
Char (single character)	'value'	middleInitial == 'D'
Float	Value (floating point literal)	average < 250.144
Enumeration	EnumName.EnumValue	

> 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 these operators and expressions:

Conditional Operators	&&, ||
Parentheses groupings and function ref-	(,), startsWith, startsWithIgnoreCase, endsWith, endsWithIgnoreCase, contains, containsIgnoreCase, in, inIgnoreCase, join, isNull, notNull, isEmpty, collectionCondition, subquery

erences	
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, if 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.

Managing Groups and Populations

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 advanced process that requires the assignment of addition IdentityIQ capabilities before these pages are displayed.

The Group Configuration page includes the following tabs:

Group Tab

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

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

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:

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.

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:

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.

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:

This information is not displayed until group aggregation is performed by a task.

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:

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

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 toa 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:

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.

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:

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.

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:

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. A workgroup email account needs to be created in your email system.

Notification Setting

Specify to whom notifications should be delivered.

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 IdentityIQ capabilities available. The capabilities currently assigned to the workgroup are highlighted on the list. 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.

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.

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.

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 and Targeted 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, allowing 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 used as Identity selection criteria for IT Role Mining activities. Groups cannot be used for IT Role Mining.