Role Management in IdentityIQ

## 

This document applies to version 7.0+, though most of its content is also relevant to previous product versions. UI navigation paths specified in this document are the 7.0+ navigation paths. The previous version of this document (found in [Role Management in IdentityIQ.pdf](https://community.sailpoint.com/docs/DOC-1643" \t "https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/_blank)​) contains the navigation path details for older IdentityIQ versions. Any other details in this document version which are applicable only to 7.0+ are specifically noted as 7.0+ features.

* [Introduction](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId-479865082)
* [Benefit of Roles](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--440085700)
* [Role Engineering in IdentityIQ](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--2040094852)
* [Role Types](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId-1334921662)
* [Organizational Roles](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--2072541953)
* [Organizational Roles as Container Roles](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId-1302474561)
* [Business Roles](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--297534591)
* [Business Role Mining](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--1217485373)
* [Managing Business Roles in the Role Navigation Hierarchy](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--329981692)
* [IT Roles](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--1929990844)
* [IT Role Mining](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId-1421955951)
* [Types of IT Role Mining Activities](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId-2112946127)
* [IT Role Mining Example: Time Tracking Application](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--1294517488)
* [Entitlement Analysis Example: Time Tracking Application](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--407013807)
* [Manual Creation of IT Roles](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId-677003379)
* [Entitlement Roles](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId-1761020565)
* [Connecting Roles to Identities](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--1646443050)
* [Assigning Business Roles to Identities](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--955452874)
* [Multiple Role Assignment to One Identity](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--264462698)
* [Detecting IT Roles](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId-819554488)
* [Linking IT and Entitlement Roles to Business Roles: Required and Permitted](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--1130201010)
* [Hard and Soft Permitted Roles](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--242697329)
* [Role Inheritance: Implications for Role Assignment and Detection](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId-841319857)
* [Different Role Types within an Inheritance Structure](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId-1532310033)
* [Certifications with Roles](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--1678640077)
* [Provisioning with Roles](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--791136396)
* [Ambiguous IT Role Profiles](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--100146220)
* [Provisioning through Roles: Multiple Account Scenario](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId-787357461)
* [Provisioning of Role Changes](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId-1674861142)
* [Propagate Role Changes Task](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--1929115978)
* [Summary of Role Change Processing](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId-416095820)
* [Role Changes on Disconnected Systems](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId-1303599501)
* [Role Change Propagation on Import](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--2103864114)
* [Partitioning and Multi-threading of the Propagate Role Changes Task](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--1216360433)
* [Role Entitlement Revocation Behaviors and Controls](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--132343247)
* [Identity Refresh Role Revocation](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId-558646929)
* [Role Lifecycle Management](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId-2035691125)
* [Role Approvals](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--1568285995)
* [Role Analytics](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--680782314)
* [Role Impact Analysis](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId-10207862)
* [Role Membership Changes](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--2136061141)
* [Role Overlap](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--1248557460)
* [Policy Validation](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--164540274)
* [Role Membership Certification](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId-919476912)
* [Certification of Role Composition](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId-1806980593)
* [Role Quality Analysis Tools](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--1600483022)
* [Role Statistics](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--909492846)
* [Direct vs. Indirect Role Association](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--218502670)
* [Business Role Statistics](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId-669001011)
* [IT Role Statistics](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId-1556504692)
* [Role Reports](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--196737301)
* [Future-Dated Role Activation and Deactivation](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId-887279885)
* [Future-Dated Role Assignment/Deassignment](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId-1578270061)
* [Role Versioning](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "toc-hId--1632680049)

# Introduction

IdentityIQ’s Role Modeler allows 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.

IdentityIQ roles are designed to be highly flexible and customizable. This flexibility allows them to be used to model a wide array of business structures and IT functions without the need for custom coding. The Role Modeler enables organizations to create roles which enforce “least privilege” access while helping to control role proliferation, a common challenge within role projects.  IdentityIQ’s role mining functionality speeds and simplifies the creation of roles that accurately represent the organization’s business and IT needs, and its role lifecycle management capabilities help organizations keep the role model up to date with changes in the business and IT structures.

This document explores how SailPoint’s role management capabilities can be used to model a real-world business and streamline identity management processes for the organization.

## Benefit of Roles

One of the major benefits 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 examine or certify this data.  Through roles, system entitlements can be grouped together and presented as a logical unit, such as a job function, rather than as a detailed and often difficult to interpret list of access rights.

In some cases, the way entitlements are expressed systematically may make it difficult for a reviewer to understand what the entitlement means. For example, groups may be specified with acronyms or numeric values which do not offer a great deal of contextual information to the layperson, and even when they 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 the data presented to the business user.

Sometimes a single job function might require multiple system entitlements, either on the same application or across multiple resources.  Without roles in place, the reviewing manager would need to know about all of the required pieces – both to understand why an employee had access to each of these and to ensure that employees were given all the access they needed 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. The responsibility for verifying and certifying the appropriate system access (the required entitlements) for that role could fall to someone else with deeper knowledge of the technical requirements.

Similarly, encapsulation of entitlements within roles also makes it possible for a manager to automatically provision the required entitlements for a new employee just by assigning that person the appropriate role (as described in [Provisioning with Roles](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "ProvRoles" \t "https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/_self) below).

# Role Engineering in IdentityIQ

SailPoint provides a comprehensive set of role engineering tools within the IdentityIQ Role Modeler which are designed to help an 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.

## Role Types

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

* ****Organizational****: organize the roles in the IdentityIQ UI for easier management
* ****Business****: identify job functions or titles or other attributes by which users can be grouped
* ****IT****: encapsulate sets of system entitlements
* ****Entitlement****: represent individual system entitlements

Custom role types can be created to model a structure that doesn’t easily fit into the IdentityIQ default model. In addition, the existing role types can be configured to function differently from their default behaviors. However, because it would be impossible to convey all the possible permutations of role structures, this document will focus only on describing various possible usages of the role structure in its default configuration.

## Organizational Roles

Organizational roles are designed for organizing the role hierarchy in the IdentityIQ UI.  As configured 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.

### Organizational Roles as Container Roles

Roles created through business and IT role mining activities (discussed in further detail in the [Business Role Mining](https://community.sailpoint.com/docs/DOC-6106/BRMining" \t "https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/_blank) and [IT Roles](https://community.sailpoint.com/docs/DOC-6106/ITRoles" \t "https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/_blank) sections) 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.

****Remember:**** 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.

## Business Roles

Business roles are typically used to represent job functions or job titles.

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:

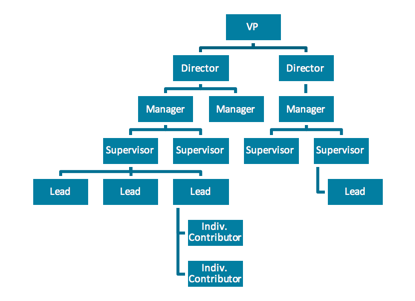
* AP Supervisor
* AP Lead Accountant
* AP Entry Clerk
* AP Mailroom Clerk

Note that even though this is a discussion of business function, the clerks’ computer system activities were considered in identifying separate business roles. In the modern, computerized world, it is inevitable that job function and system access are tightly coupled. Although it is valuable – even important – to consider system access when defining business roles, be aware that system entitlements will not actually be directly associated with the business roles in IdentityIQ’s default role model. The entitlements themselves will be encapsulated in IT roles (as described in [IT Roles](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "ITRoles" \t "https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/_self)), which are then linked to the business roles.

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

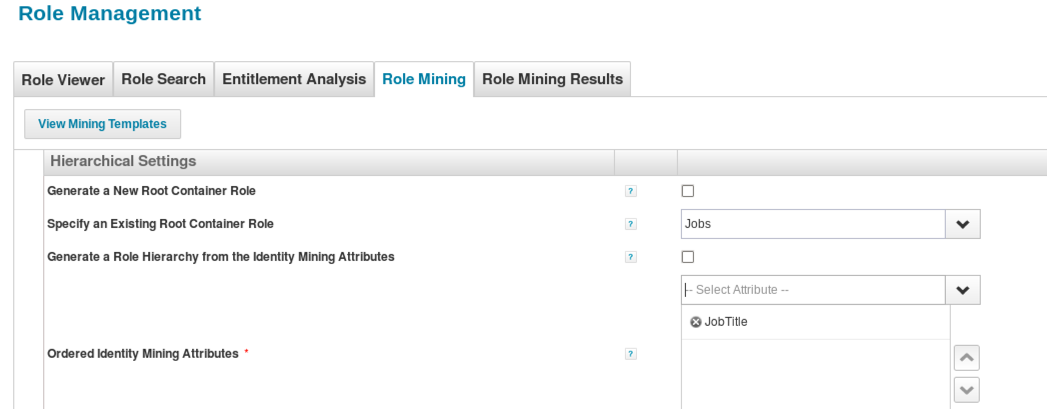
So any division within the company might look something like this:



In this case, it might be desirable to create a set of business roles to represent the position levels for the management and supervisory positions: VP, Director, Manager, Supervisor, and Lead. This is particularly valuable if there are business tasks, especially ones connected to system-access needs, that must be performed by all people who share the same position title; for example: all Supervisors are responsible for approving time entries in a company-wide time-tracking system. However, if the titles are only used to represent pay grade or relative position in the company, such that Managers in Finance and Managers in Operations have no common responsibilities, this level of role representation may ultimately only add complexity and serve no valuable purpose in Identity management. This sort of analysis is a major part of the role definition process and is critical to successfully and usefully modeling the organization’s business activities in a role structure.

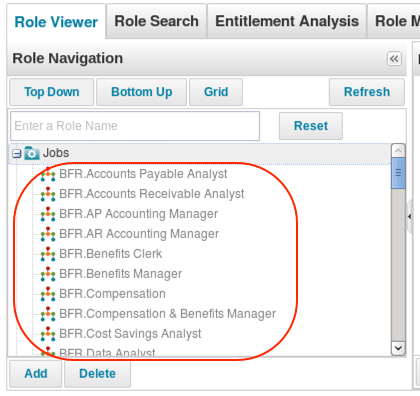
### Business Role Mining

Though business roles can be manually created through the IdentityIQ user interface, role mining can also be used to generate business roles and can often do the task much more efficiently than a manual process. 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****.



Even if the final set of business roles is only loosely related to a specific attribute, starting with a generated set of roles based on key attributes can save time in the role creation process; editing and manipulating mined roles can still be faster than manually generating them all. Consider the AP Clerk example. Perhaps the official job title for the Mailroom Clerks and the Entry Clerks is simply “AP Clerk.”  Even if role mining only creates 3 roles: AP Supervisor, AP Lead, and AP Clerk, the AP Clerk role can be cloned and edited to create both the AP Mailroom Clerk and AP Entry Clerk positions.

Role mining can also minimize the risk of missing roles. Manually creating a list of job titles could easily result in a few omissions, particularly in large organizations with lots of different job titles. An automated role mining activity would find and create a role for every job title assigned to any Identity.

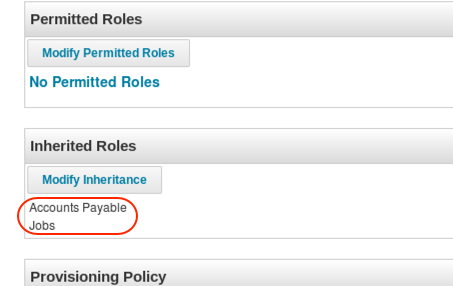


****NOTE****: Mined business roles are created in a disabled state and must be activated before they can be assigned to any identity, either automatically or through an access request.  Mined business roles also automatically contain assignment logic which will automatically assign them to identities whose attributes match the criteria used to identify the role, once the role is activated.

### Managing Business Roles in the Role Navigation Hierarchy

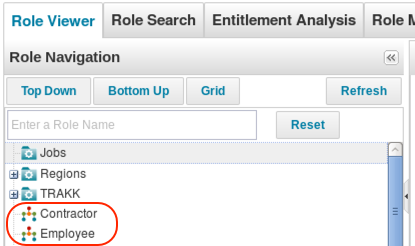
The position of roles in the UI role hierarchy is controlled by inheritance.  When business roles are generated through mining, they are created in a container role.  They can be left in this container, moved to another organizational role (such as one representing the corporate division or department to which the role belongs), or shown in multiple places by inheriting from the original container and other organizational roles.

To connect a business role to a new organizational role, add the organizational role to the ****Inherited Roles**** section of the business role definition. This makes the organizational role a “parent” to the business role, in the top-down hierarchical view.  To remove it from the original container, delete that role from the ****Inherited Roles**** list.  Alternatively, to link the business role to more than one organizational role and therefore show it multiple places in the hierarchy, add all of the organizational roles to the business role’s ****Inherited Roles**** list.  This sort of structure could be used to denote that a business role applies to more than one branch of the organizational hierarchy or simply to include it in an org hierarchy while also retaining it in the role mining container for easier ongoing management.



Note that while the role appears to exist in multiple places in the role navigation structure, all references to it point to the same actual role so making changes in one part of the role hierarchy changes that role everywhere it is linked. As a result, the administrator can manage changes to a role from the any part of the role tree and affect the role everywhere it is visible.

Finally, while business roles are often contained within one or more organizational roles, they do not have to exist within any organizational role framework. When roles do not inherit from any other role, regardless of the type of role they are, they appear at the top level of the hierarchy in the ****Top Down**** view in the ****Role Navigation**** pane.



## IT Roles

IT roles allow multiple entitlements from one or more applications to be grouped together into a single role. Creating the right set of IT roles is probably one of the most critical and difficult parts of configuring the role structure.  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; this can be more of an art than a science.

### IT Role Mining

In general, the most efficient way to get started creating IT roles in the IdentityIQ Role Modeler is to generate them through role mining. In role mining, IT roles are generated based on system access current employees already have.

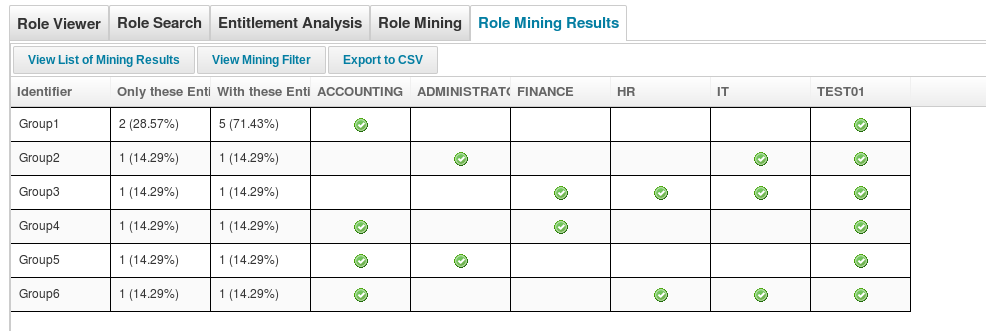
#### Types of IT Role Mining Activities

Roles can be mined either by performing an ****IT 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:

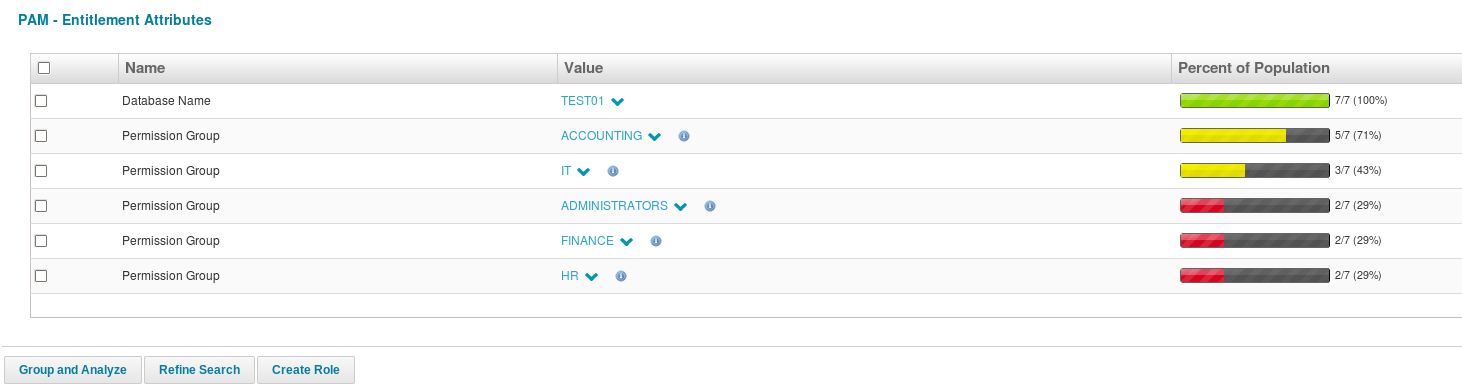
* Both allow the administrator to specify one or more applications whose entitlements will be evaluated as well as a set of identity attributes that can be used to filter the set of Identities that should be examined.
* Both only return entitlements held by at least one identity in the examined set.  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.



     IT Role Mining



     Entitlement Analysis

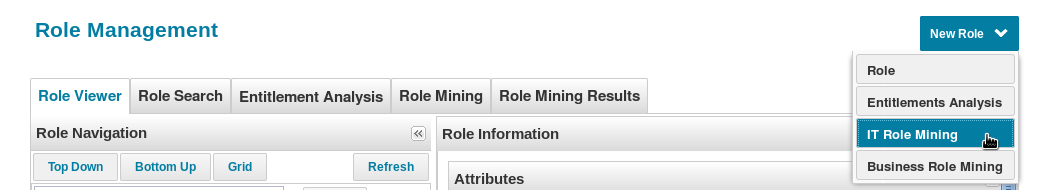
Two other administrative differences exist between these two role mining options:

* IT Role Mining definitions and results can be saved to be re-run or examined later.  In Entitlement Analysis, neither the results nor the criteria specified are saved once the administrator leaves the Role Management area of IdentityIQ; all role creation from the analysis must be done at once or the analysis must be re-run.
* Roles created from IT Role Mining are created in a disabled state and must be enabled before they will be detected for any user.  Entitlement Analysis roles are created in an enabled state and will be detected for users in the next identity refresh task execution (with the appropriate options selected).

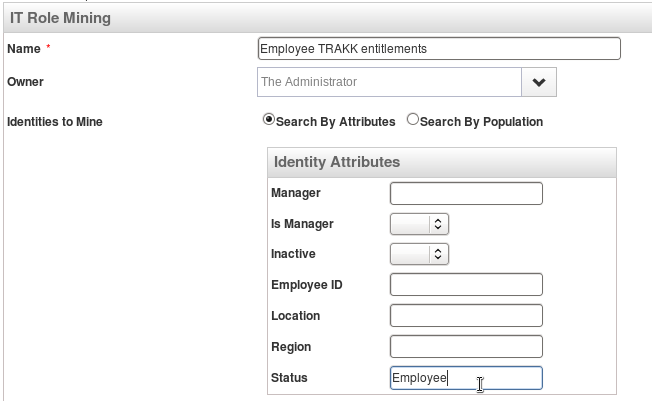
To provide a clearer picture of how IT roles can be structured and how the mining activities can help with that process, the two examples below illustrate a real-world IT role a company might create and how role creation would be done through each of the IT role mining options.

#### IT Role Mining Example: Time Tracking Application

Consider, for example, a time-tracking application that is in use across the company by all employees, though not by contractors.  On the ****Role Management**** window (****Setup**** -> ****Roles****), select ****IT Role Mining**** from the ****New Role**** drop-down list.



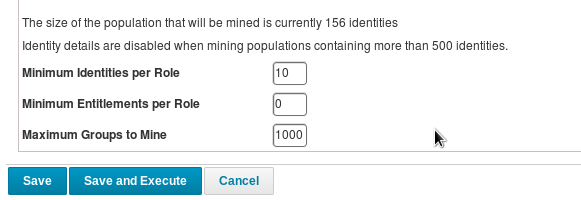
Specify any desired Identity attribute filters or select a population as the Identity filter criteria.  For example, to run a role mining task for only employees, specify (Identity Attribute) ****Status****=****Employee****.



Next, select the application(s) to mine, and if desired, select any entitlements on that application to exclude from the mining activity.  This example mines the TRAKK application and excludes no entitlements.

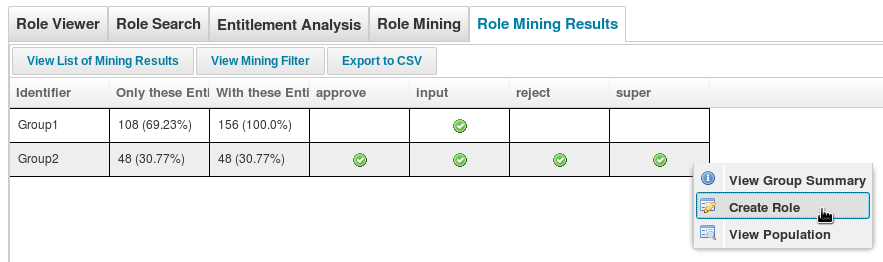


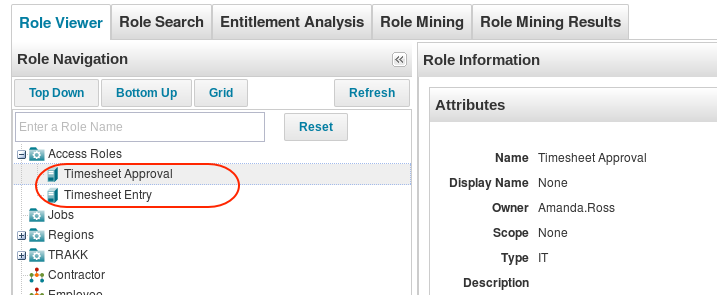
To restrict role identification based on a minimum threshold of Identities or entitlements or to cap the total number of groups, specify those constraints in the mining activity definition.



Click ****Save and Execute**** to run the mining activity immediately.

This role mining activity shows that 100% of the population has “input” access to the time tracking system and that a second population additionally has “approve”, “reject”, and “super” capabilities. Right-click each group record and click ****Create Role**** to create an IT role with capabilities that match those identified for the group (IT Roles ****Timesheet Entry**** and ****Timesheet Approval****).



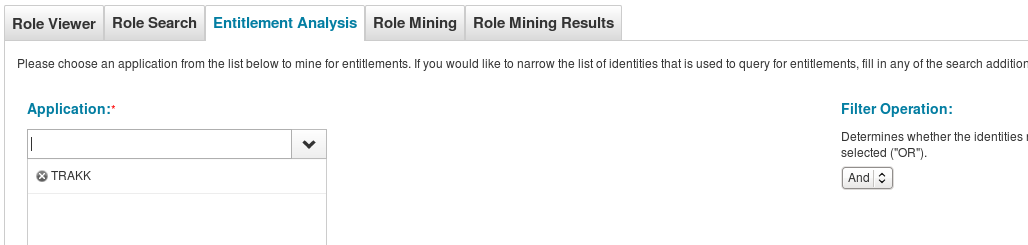


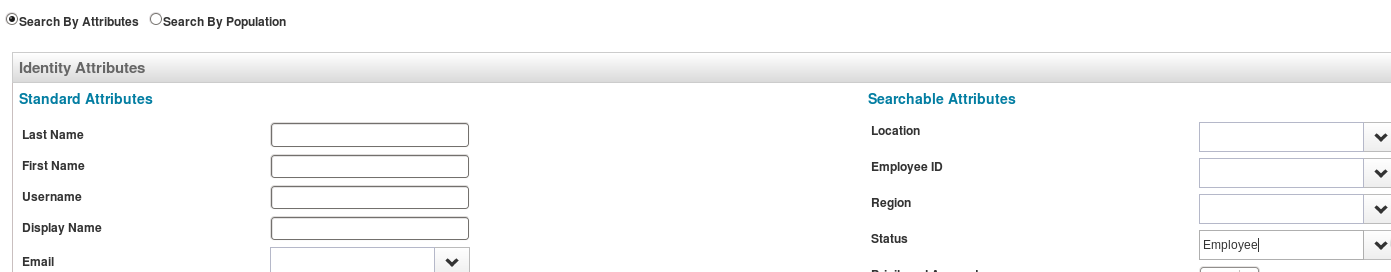
Notice that a container role (called ****Access Roles**** in this example) is used for IT role mining, just as it was with business role mining. As with the business roles, the container can be a temporary tool or can permanently house the generated set of IT roles. In fact, it is more likely that IT roles will be left permanently recorded within their container role because they generally do not inherit from the business roles to which they are associated. Instead, they are linked to the business roles as ****Required**** or ****Permitted**** roles for the business role (see [Linking IT and Entitlement Roles to Business Roles](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "Linking" \t "https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/_blank)).

****NOTE****: While the IT Role Mining process for this application only identifies the two groups of entitlements, these groups can be used to create multiple roles by editing the included entitlements list during the role creation process.  It is also possible to redefine the mining activity to exclude certain entitlements so additional groups will be revealed and available for role creation.  For example, to see statistics on and create a role representing the approval and rejection entitlements only, change the mining definition to exclude the “input” and “super” entitlements and re-run the role mining activity.

#### Entitlement Analysis Example: Time Tracking Application

This same set of time-tracking roles could alternatively be created through an Entitlement Analysis.  From the Role Management window (****Setup**** -> ****Roles****), click the ****New Role**** drop-down list and click ****Entitlement Analysis****.  Select the ****TRAKK**** application and specify a filter of ****Status**** = ****Employee****.



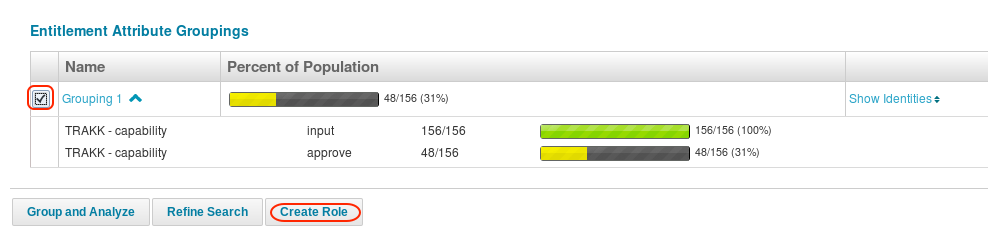


Click ****Search**** to run the analysis.

The results show the four individual entitlements available on the TRAKK application, along with the percentage of Identities in the examined set (those with an account on TRAKK and Status = Employee) who have each of those entitlements.  The entitlements are not pre-grouped into sets and the administrator can choose to group them in any way to create roles.  For example, the administrator could easily create a role made up of the “input” and “approve” capabilities only.  Though the current set of users either have all capabilities or just “input”, future users could have other combinations of entitlements, and this option allows roles to be created for any desired combination.  While this presentation style is more flexible, it does not highlight the combinations of entitlements held by current users as well as the IT Role Mining task does.

To create a role as a combination of entitlements, first select the checkboxes for each of the desired entitlements and click ****Group and Analyze****.  Then select the checkbox on the generated grouping and click ****Create Role****.

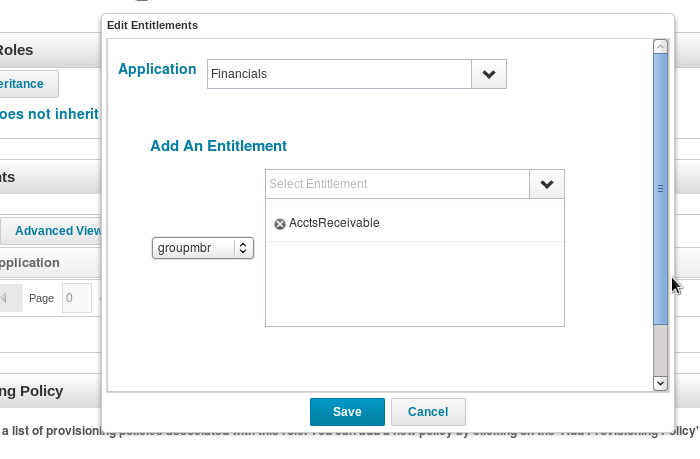


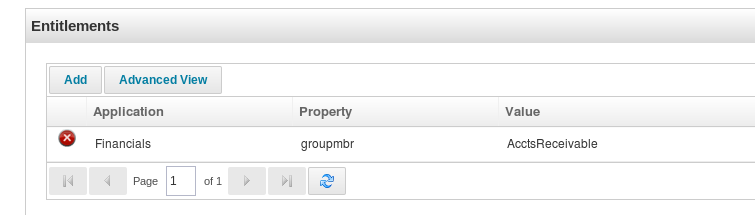


### Manual Creation of IT Roles

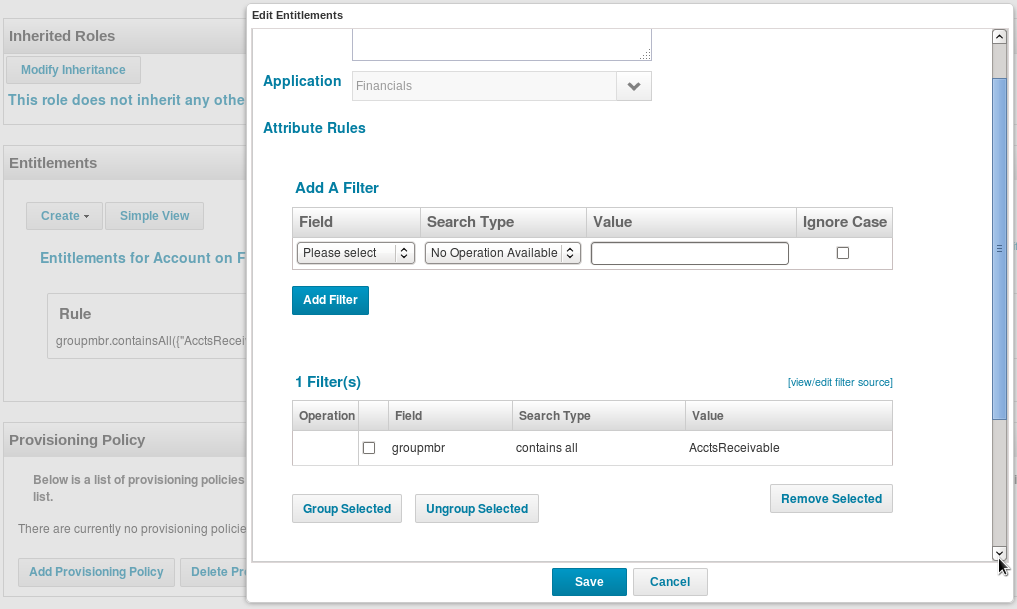
In addition to these automated role creation options, IdentityIQ also allows an administrator to manually create IT roles through the user interface. This option is most frequently used when the role structure is already known and available in some other form or repository; the IT roles can be manually entered or brought into IdentityIQ through a direct load process. When the roles are not already defined, however, role mining is usually a much more efficient method of driving the IT role creation process than manual entry.

The most important step in manually creating these roles is defining the Entitlements they contain. Entitlements are recorded in a “profile” in the role definition.  In simple terms, the “profile” specifies the entitlements assigned to a role.  In fact, the user interface presents the selection of entitlements in just that way in its ****Simple View**** (default view): the user selects entitlements and directly assigns them to the role.  All entitlements added to the role are required for the role (i.e. they are connected in a simple “and” relationship).

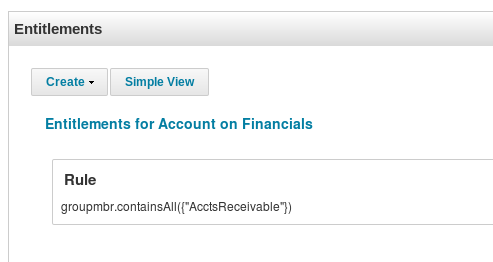




The ****Advanced View**** is available for creating more complex profiles. For example, it allows specification of a profile involving an “or” condition, in which any one of several entitlements can be used to detect the role rather than requiring all of the entitlements to be present at once.  It can also be used to specify a role profile with a combination of “and” and “or” relationships.



Instead of a list of Entitlements, the ****Advanced View**** of the profile shows the exact syntax of the filter string that will be used to match the Identities to the role in the detection process.



Once defined through either view, the entitlement profile is used to detect the presence of these roles for an Identity and to provision these roles when they are part of the required or permitted roles list of an added business role.  More information on how the profiles are used can be found in the [Detecting IT Roles](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "DetectITRoles" \t "https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/_blank) and [Provisioning with Roles](https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/77726" \l "ProvRoles" \t "https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/_blank) sections below.

## Entitlement Roles

Entitlement roles were originally created to represent a single entitlement on a single application.  They were created by the ****Entitlement Role Generator**** task, which can run against one or more applications, examining one or more attributes and/or permission targets, and creating as many roles as are required to represent each entitlement value with a separate role.  The primary value in this was to support adding meta-data such as owners, descriptions,  display names, and extended attributes to individual entitlements.  Since version 6.0, the Entitlement Catalog supports all of those data points on individual entitlements directly, so entitlement roles have been rendered obsolete.  Today, Entitlement roles exist for backward compatibility and are not recommended for current/new installations. Furthermore, employing too many entitlement roles can result in role proliferation that gets in the way of roles’ usefulness.

Installations pursuing a roles-only authorization structure may be drawn to this role type when they identify individual entitlements which stand alone as their own role.  However, this same functionality could be achieved by creating an IT role with only one entitlement; in fact, the default configuration for entitlement roles exactly matches that of IT roles, making them completely interchangeable.  The approach of using IT roles for these single-entitlement roles avoids the introduction of a different type of role configured with its own set of default behaviors, though it may still result in creating a high volume of roles if these single-entitlement-role scenarios are common.  Most organizations will choose to manage these one-off entitlements just as entitlements and use roles only when grouping sets of multiple entitlements together.

## Connecting Roles to Identities

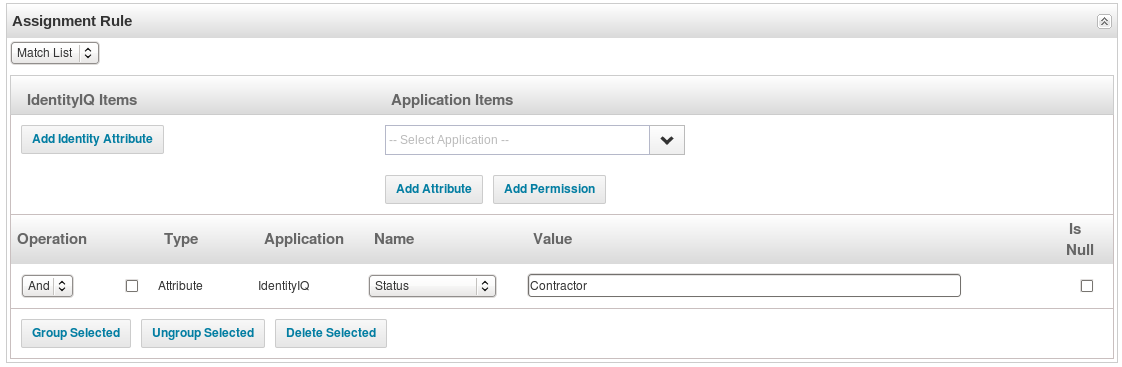
The purpose of creating all these roles is to facilitate managing entitlements for Identities, so of course the roles must somehow be connected to the Identities. Roles can either be “assigned” to an Identity or “detected” for an Identity, as described below.

|  |  |  |
| --- | --- | --- |
| ****Term**** | ****Definition**** | ****Applicable Role Types****  **(default configuration)** |
| Assigned Role | A role that has been explicitly linked to an Identity, either manually through the IdentityIQ user interface or by application of an “assignment rule” written for the role | Business Roles |
| Detected Role | A role that is been deemed applicable (and therefore linked) to an Identity because all the entitlements associated with that role are held by the Identity. | IT Roles |

In the default configuration of IdentityIQ roles, only business roles can be “assigned” to Identities. By contrast, IT roles are “detected” for an Identity based on its recorded system entitlements.

### Assigning Business Roles to Identities

Business role can be manually or automatically assigned to each Identity. 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, execute a ****Refresh Entitlement Correlation**** task or an Identity Refresh task with the ****Refresh assigned, detected roles and promote additional entitlements**** option selected.

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 (see [Filters and Filter Strings.pdf](https://community.sailpoint.com/docs/DOC-1628" \t "https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/_blank)​ for more information on this syntax)
* ****Script**** / ****Rule****: beanshell code that specifies 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

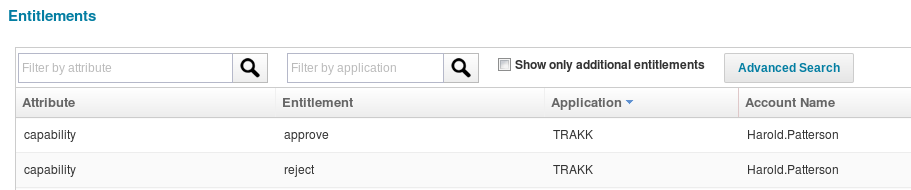
****NOTE****: If role-mining-generated roles are manually modified, the assignment rules generated for them may no longer apply.  In that case, the assignment rules must be edited as well to prevent them from being incorrectly assigned to Identities.

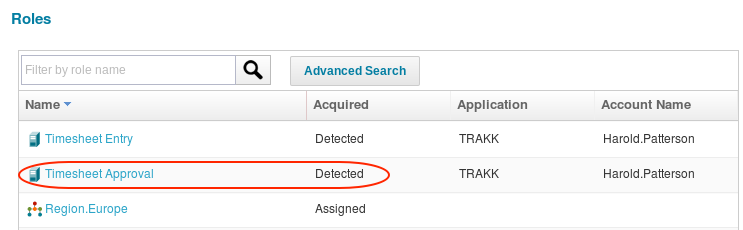
#### Multiple Role Assignment to One Identity

Beginning in version 6.3, IdentityIQ supports assignment of one role to the same identity multiple times.  This is relevant, and important, when a user has multiple accounts on an application and needs to have a role assigned to grant required access to more than one account.  Only one instance of the role will be auto-assigned through this assignment rule logic, but a second (or third, etc.) instance can be requested for the user through a role request in Lifecycle Manager.  Additionally, this same feature set allows targeting of the role's entitlements to a specific account so that the access can be specifically managed per account.  See the [Roles and Multiple Accounts](https://community.sailpoint.com/docs/DOC-3260" \t "https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/_blank) white paper for more details on the configuration and requirements for supporting multiple role assignment.

### Detecting IT Roles

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.)





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

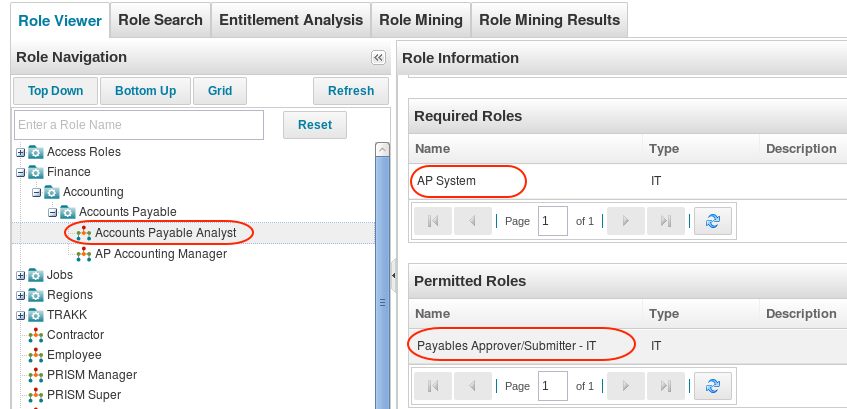
In role detection, IdentityIQ compares the entitlement profiles of each role to the entitlements held by each Identity. Profiles may specify a single entitlement or may specify multiple entitlements, either in “and” relationships, requiring the identity to have all listed entitlements to have the role, 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.

### Linking IT and Entitlement Roles to Business Roles: Required and Permitted

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

* A business role’s ****Required Roles**** are the IT roles that an Identity must have when they are associated with that business role.
* Its ****Permitted Roles**** are the ones that the Identity can have but is not required to have when assigned that business role.

Another way to look at this is: Required IT roles are ones the user must have to do their job; Permitted IT roles are ones the user can have but does not have to have when they are assigned the business role.  This may be because the permitted IT role’s entitlements are more privileged or because its entitlements are simply less widely required.  For example, an Accounts Payable Analyst must have the AP System role, which represents basic access to the accounts payable system, but they may only require (or be allowed to have) the Payables Approver/Submitter role if that task is part of their specific job duties.  Likewise, a System Developer must have access to the Source Code Control System to do his job. He may have access to the VPN to be able to work remotely, but that access is not required. The source code system IT role would be a Required Role while VPN Access would be a Permitted Role.



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 (see [Provisioning with Roles](https://community.sailpoint.com/docs/DOC-6106/ProvRoles" \t "https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/_blank) for more information). 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.

### Hard and Soft Permitted Roles

IdentityIQ version 6.3 introduced a new distinction in how permitted roles can be granted to users in relation to business role assignments.  The presence of permitted roles can now be associated to business role assignments through “hard permitted” and “soft permitted” relationships.

* ****Hard permitted**** roles are permitted roles held by an Identity which were explicitly requested as part of a business role request.
* ****Soft permitted**** roles are permitted roles which were not explicitly requested but have been identified as held by an Identity through role detection and have been associated to a permitting business role through defined “permits” role relationships.

Soft permitted roles are displayed in the UI as connected to the business roles which allowed them, but since they were not specifically granted by the request for the business role, they are treated as separate entities whose association to the Identity is not controlled by the business role assignment.  Consequently, when the business role is revoked from a user by an automated process, any soft permitted roles – and their underlying entitlements – are left in place for that user.

Prior to 6.3, all permitted roles were treated like soft permitted roles are now. This was because IdentityIQ did not keep track of whether permitted roles were included in a role request.  Since the system did not know whether a permitted role’s entitlements were added to the Identity cube as a result of a specific access request or whether they were simply detected there based on the Identity’s held entitlements, it would have been inappropriate for an automated procedure to revoke those entitlements.

Starting with version 6.3, however, IdentityIQ tracks when permitted roles are requested as part of a business role request.  When they are, the relationship between the business role and the permitted IT role is reflected on the Identity cube, and the role is said to be a “hard permitted role”.  All IT roles, whether required, permitted, or just found present, are represented in the Identity XML as RoleDetection objects when they are discovered for an Identity.  Hard permitted roles are additionally represented in the Identity’s XML representation as a nested list of role assignments under the parent business role assignment as PermittedRoleAssignments entries like this:

<RoleAssignment assigner="spadmin" assignmentId="4fe93bb6c413456c9152279c9b435235" date="1405053338986" roleId="40288083472139f10147213a198d000f" roleName="ACC Portal" source="LCM">

  <PermittedRoleAssignments>

      <RoleAssignment assigner="spadmin" date="1405053338986" roleId="40288083471c096701471f9d05f9026b" roleName="ACC Portal Document Read"/>

      <RoleAssignment assigner="spadmin" date="1405053338987" roleId="40288083471c096701471f9f1b4c026e" roleName="ACC Portal Document Write"/>

   </PermittedRoleAssignments>

   <RoleTarget applicationId="4028808346f1e1b50146f1e20bcc0295" applicationName="Sailpoint LDAP VM" nativeIdentity="cn=Alan.Bradley,ou=people,dc=training,dc=sailpoint,dc=com" roleName="ACC Portal Document Read"/>

   <RoleTarget applicationId="4028808346f1e1b50146f1e20bcc0295" applicationName="Sailpoint LDAP VM" nativeIdentity="cn=Alan.Bradley,ou=people,dc=training,dc=sailpoint,dc=com" roleName="ACC Portal Access"/>

   <RoleTarget applicationId="4028808346f1e1b50146f1e20bcc0295" applicationName="Sailpoint LDAP VM" nativeIdentity="cn=Alan.Bradley,ou=people,dc=training,dc=sailpoint,dc=com"/>

</RoleAssignment>

Since this data is now tracked, it can be used to drive automatic remediation.  Any IT role which is hard permitted by a business role will therefore be automatically revoked when its permitting business role is revoked in an automated process.

****NOTE****: Any permitted role – hard or soft -- can be selected for removal through a certification or in an LCM request.  This change relates only to automated revocation processes (e.g. role changes based on assignment rule logic in an Identity Refresh task).

## Role Inheritance: Implications for Role Assignment and Detection

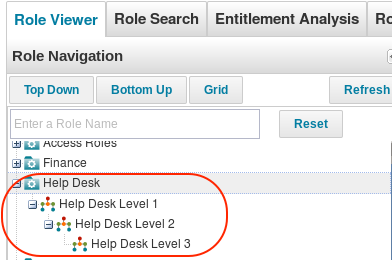
In some organizations, business roles or IT roles can be efficiently modeled using an inheritance-based role structure.

Business roles are 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. In essence, Help Desk Level 2 can be considered a special case of Help Desk Level 1 and Help Desk Level 3 can be seen as a special case of Level 2.

|  |  |
| --- | --- |
| ****Support Level**** | ****Assigned Tasks**** |
| 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.”

This structure is ideally suited to modeling with role inheritance.



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.

The assignment rule criteria for these roles, then, would be:

|  |  |
| --- | --- |
| ****Role**** | ****Attribute Details**** |
| Help Desk Level 1 | Department = "Help Desk" |
| Help Desk Level 2 | Location = "Denver" |
| Help Desk Level 3 | JobTitle = "Senior Engineer" |

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.

This table shows how the roles would be assigned for this set of Identities with these attribute values.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ****Identity**** | ****Department**** | ****Location**** | ****Job Title**** | ****Role Assigned**** |
| George.Wright | Help Desk | Denver | Senior Engineer | Help Desk Level 3 |
| Clarence.Harper | Help Desk | Porto Alegre | Support Engineer | Help Desk Level 1 |
| Betty.Young | Help Desk | Denver | Support Engineer | Help Desk Level 2 |
| Marilyn.Dunn | Help Desk | Toronto | Senior Engineer | Help Desk Level 1 |
| Mark.Allen | Help Desk | Denver | Senior Engineer | Help Desk Level 3 |
| John.Smith | Finance | Denver | Financial Analyst | [none of these] |

Note that Marilyn.Dunn’s attributes actually match the criteria for Level 1 and Level 3. She is assigned Level 1 because the inheritance structure requires that she also match Level 2’s criteria to be considered for Level 3. She is not in the Denver location, so she does not meet the criteria for Level 2 or, through inheritance, Level 3.

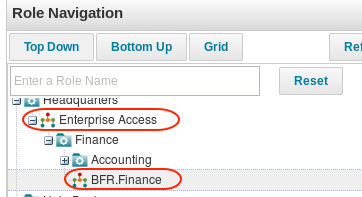
As an interesting aside, if Help Desk Level 2 were set up but contained no assignment rule of its own, the fact that it inherits Level 1’s assignment rules and is deeper in the hierarchy means that all Identities meeting the Level 1 criteria would actually be assigned the Help Desk Level 2 role instead, and no Identities would be assigned the Level 1 role.

****NOTE****: Any required and permitted IT roles listed for each level are also passed on to their inheriting roles. This means that all required roles for Help Desk Level 1 personnel are also required roles for Help Desk Level 2 and Level 3 personnel as well.

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.

### Different Role Types within an Inheritance Structure

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. For example, in the hierarchy pictured below, assignment rules and required/permitted IT roles specified for the Enterprise Access business role are not inherited by the BFR.Finance business role within the Finance Organization, even though they are related through an inheritance structure. 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.



An Identity who needed the Enterprise Access and the BFR.Finance roles would have to be explicitly assigned both roles in this scenario.

## Certifications with 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.

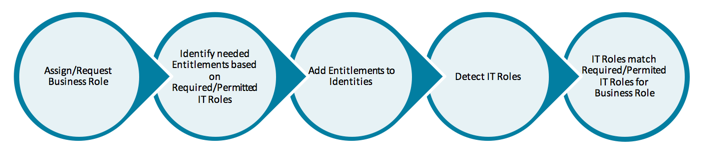
## Provisioning with Roles

A well-designed role structure greatly simplifies provisioning of entitlements for Identities. The provisioning request itself usually centers on the Business role, whether it is initiated through a Lifecycle Manager request or by automatic assignment logic.  Lifecycle Manager role requests are usually for business roles that are associated with the job functions the user needs to perform; role assignment rules usually assign a business role based on identity attributes that connect the user with the job function the role represents.

When a new business role is assigned to an Identity, the IT roles connected to it as required and permitted roles are examined. The entitlements associated to the required roles will be provisioned for the Identity; the permitted roles’ entitlements are provisioned only of they are specifically requested for the Identity.  Lifecycle Manager automatically prompts the requester to decide whether to request the permitted roles or not.  Automatic role assignment based on assignment rules does not auto-provision permitted roles, so in that case, permitted roles (and therefore the associated entitlements) must be requested separately for the user.

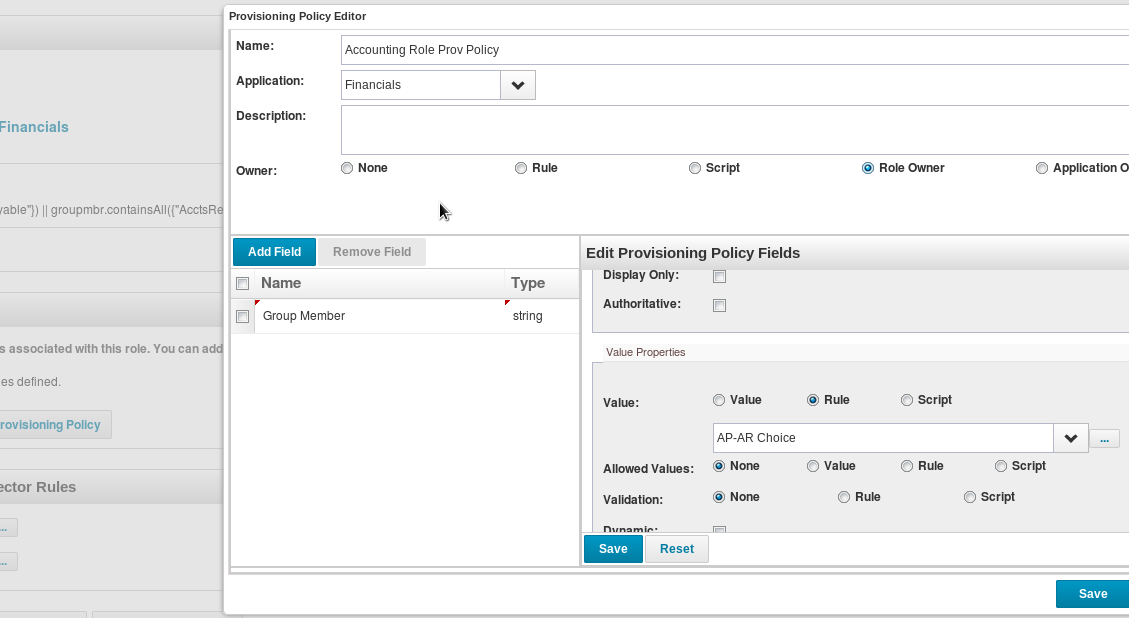
****NOTE****: When a role is requested for a user through Lifecycle Manager, the provisioning request for the role itself and for any underlying entitlements granted by the required or permitted IT roles begins processing immediately (unless explicitly scheduled for fulfillment at a later date).  However, when a business role is added to an Identity through an assignment rule, run by an Identity Refresh task, the provisioning request for the entitlements granted by the business role’s required or permitted IT roles is not always submitted automatically.  That request is created by an Identity Refresh task with the ****Provision Assignments**** option selected.  This could be done by the same Identity Refresh task that assigns the business role or could be performed in a separate Identity Refresh task execution, depending on the options chosen in the task configuration.

The diagram below illustrates, at a high level, the progression that occurs from the time a new business role is requested until IdentityIQ has identified that all of the corresponding IT roles and entitlements are correctly associated to the Identity. Note that it is still through detection of the added entitlements that the IT role is linked to the Identity; IT roles are not assigned to the Identity directly. (The specifics of provisioning execution differ depending on the request mechanism and the provisioning configuration in place, but the core process remains the same.)

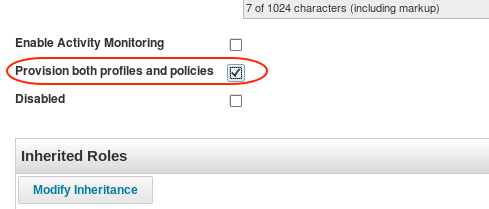


### Ambiguous IT Role Profiles

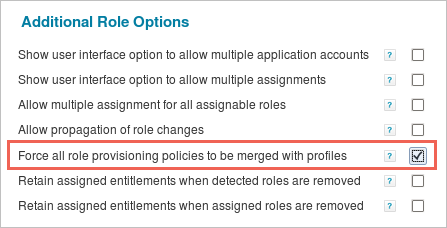
When provisioning a required or permitted IT role with an “or” profile, additional information is needed to complete the request.  This is because an “or” profile inherently allows more than one entitlement to fulfill the requirement, and it is inherently unclear which entitlement must be provisioned.  To disambiguate the profile, a role Provisioning Policy is needed.  The ****Provisioning Policy**** can automatically determine which entitlement to provision by looking at available identity attributes or it can require a person (e.g. the requester, role owner, etc.) to make the determination.



The ****Provision both profiles and policies**** option specifies that the provisioning policy provides supplemental information to the profile and that the profile should still be used to define some parts of the provisioning request.  When this option is not selected, a provisioning policy added to a role causes the profile to be ignored entirely in the provisioning process, so the provisioning policy must contain all of the information needed for the provisioning request.



However, there is a system configuration that overrides this and forces the default provisioning behavior for all roles to be based on both profiles and policies.  On the gear menu -> ****Global Settings**** -> ****IdentityIQ Configuration**** -> ****Roles**** page, under ****Additional Role Options****, select the option: ****Force all role provisioning policies to be merged with profiles****.



### Provisioning through Roles: Multiple Account Scenario

IdentityIQ (versions 6.3+) supports provisioning of entitlements through roles when the target user has multiple accounts on an application.  This scenario most commonly arises when an individual has a regular user account and an administrator account on an application, though the functionality is not limited just to that situation.

This functionality allows a target account to be selected at the time of role provisioning, and where desired, allows assignment notes to be entered which explain the account selection.  It also allows IdentityIQ to support multiple assignment of a role to the same identity, targeting different accounts in each assignment. A separate white paper, called [Roles and Multiple Accounts](https://community.sailpoint.com/docs/DOC-8559" \t "https://community.sailpoint.com/t5/Technical-White-Papers/Role-Management-in-IdentityIQ/ta-p/_blank), contains the details of the configuration and requirements for using this functionality.

### Provisioning of Role Changes

A role’s definition can change after it has been created and assigned to identities.  It is important to understand how those changes affect the associated identities’ entitlements. New functionality was introduced in this area in version 6.4: namely, a task for pushing role changes to identities which hold those roles.

#### Propagate Role Changes Task

The Propagate Role Changes task was introduced in version 6.4 to manage 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. Navigate to theIMG_287gear menu -> ****Global Settings**** -> ****IdentityIQ Configuration**** -> ****Roles**** page and select ****Allow propagation of role changes****. This turns on the creation of RoleChangeEvents, which record changes to the composition of any role.
2. Create a task of type ****Propagate Role Changes**** (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.

****NOTE****: Both identity refresh tasks and this propagate role changes task can propagate additions to role definitions.  In 6.4, this propagation task is single-threaded while identity refresh tasks can be partitioned, so when propagating additions to role definitions which affect large percentages of the identity population, an identity refresh task will be substantially more performant in pushing out the changes.  However, in 7.0+, the propagation task also became a partitioned task which could take advantage of multiple threads on multiple hosts to process the role changes.  In either version, If a role entitlement addition will affect only a small percentage of the identity population, using the role propagation task to push out the role change will be more efficient than running a full refresh of all identities. Also, note that entitlement removal from a role definition can only be processed by this propagation task, not by a refresh task.

#### Summary of Role Change Processing

The table below describes what occurs in various role change scenarios in IdentityIQ.

|  |  |
| --- | --- |
| ****Scenario**** | ****Result**** |
| User has an assigned business role.  A new required IT role is added to the business role definition. | An Identity Refresh task, with Provision Assignments selected, provisions the entitlements in the new required IT role for the identity.  The Propagate Role Changes Task can also provision these entitlements. |
| User has an assigned business role.  New entitlements are added to an IT role required by that business role. | An Identity Refresh task, with Provision Assignments option selected, provisions the new entitlements for the identity.  The Propagate Role Changes Task can also provision these entitlements. |
| User has an assigned business role.  An IT role is removed from the Required Roles list. | Prior to version 6.4, no update is made to the identity’s entitlements.  Identity Refresh does not remove entitlements based on role definition changes.  In version 6.4+, the Propagate Role Changes Task deprovisions the no-longer-required IT role entitlements for the identity. |
| User has an assigned business role.  Entitlements are removed from a Required Role’s entitlement profile. | Prior to version 6.4, no update is made to the identity’s entitlements.  In version 6.4+, the Propagate Role Changes Task deprovisions the entitlements for the identity. |
| User has an assigned business role.  A permitted IT role was requested for the user because of or during the business role assignment.  New entitlements are added to the permitted IT role. | In 6.2+, this requested permitted role is marked as “hard permitted” so an Identity Refresh task with Provision Assignments selected provisions the new entitlements in the permitted IT role for the identity.  The Propagate Role Changes Task will not do this provisioning because that task only applies to required roles. |
| User has an assigned business role.  A permitted IT role was requested for the user because of or during the business role assignment.  Entitlements are removed from the permitted IT role. | The entitlements remain associated to the identity even though they are no longer part of the role, even after an identity refresh or a role propagation task in 6.4+.  Identity refresh does not remove entitlements based on role definitions and the role propagation task only operates on required IT roles.  However, the entitlements are now “additional entitlements” and will be displayed and certified independently from any role association. |
| IT role is detected for a user based on their currently held entitlements; there is no business role assigned to the user which requires that IT role.  New entitlements, which the user does not yet have, are added to the IT role. | The IT role is no longer detected for the identity.  The user does not have the required entitlements so the role cannot be detected for them, and no provisioning of the entitlements occurs since the IT role is not required by a business role assigned to the user. |

#### 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 results 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 exposed in the UI-based task options 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.

With the role propagation task, no such option exists.  Instead, in the role propagation task, you have the option of having the task run a workflow in which you can do whatever you choose (including forcing the creation of manual work items). That workflow 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 cert could then trigger manual provisioning work items to process additions, or an informed certifier could revoke the no-longer-required extra access.

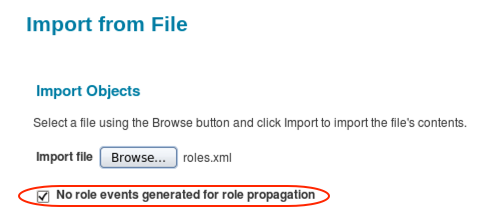
#### Role Change Propagation on Import

In version 6.4, the role change propagation functionality was only available for changes made through the Role Editor in the IdentityIQ user interface.  Role changes which were imported, either through the iiq console or through the UI ****Import From File**** option, did not generate RoleChangeEvent objects and therefore did not get propagated to identities which held those roles.  Versions 7.0+ implement the role change propagation functionality for imported role changes.

In circumstances where a customer wants to import role changes or new role definitions without creating role change events and spurring role propagation, they must specify 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 user interface's ****Import from File**** page (gear menu -> ****Global Settings**** -> I****mport from File****) suppress role change event creation by selecting the option ****No role events generated for role propagation****.



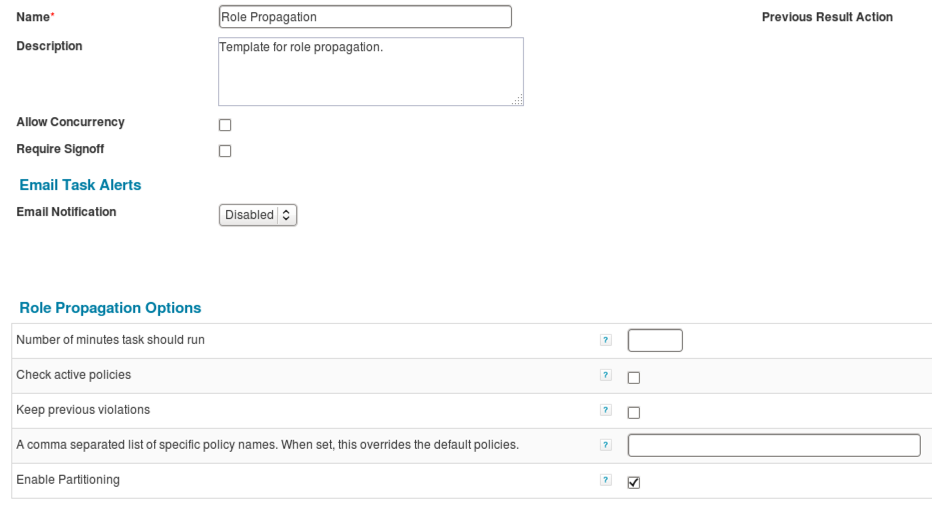
#### Partitioning and Multi-threading of the Propagate Role Changes Task

Version 7.0 introduced multi-threading to the Propagate Role Changes task, increasing its flexibility and improving its performance.

Partitioning of this task depends on these configurations:

1. A Propagate Role Changes task with partitioning enabled
2. A number of partitions configured in the role propagation task or a calculation of the number of partitions based on:
   1. The maxThreads value specified in the Role Propagation Partition RequestDefinition object and
   2. The maxRequestThreads value (optionally) specified in each Server object, representing the maximum number of threads to use on that server for processing requests

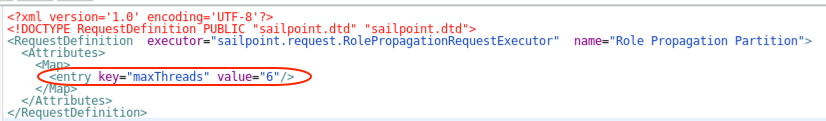
To use partitioning with role propagation, first select the ****Enable Partitioning**** option in a task of type ****Propagate Role Changes****.



To force the system to use a specific number of partitions for the task, edit the configured task definition through the Debug pages to add a ****partitions**** argument specifying the number of partitions to use.



Alternatively, allow the system to auto-calculate the number of partitions.  This calculation relies on values in the ****Role Propagation Partition**** RequestDefinition object and the Server objects for each host configured as a Request host.  The ****maxThreads**** argument in the Role Propagation Partition RequestDefinition should specify the maximum number of threads to use for this process on any host.  The ****maxRequestThreads**** value in each Server definition should specify the maximum number of threads to use for request processing on that specific host.  The lesser of these two values will be used as the partition count for each server in the partitions calculation.





For example, consider an environment with 2 hosts, one which can handle up to 8 concurrent threads and another which can handle only 4.  If maxThreads for role propagation were set at 6 and the hosts have their maxRequestThreads values set at 8 and 4, respectively, then the partition count for this task would be calculated as 6 + 4, or 10. The RequestDefinition maxThreads constrains the partition count for the larger host and the Server's maxRequestThreads constrains the partitions for the smaller host.

### Role Entitlement Revocation Behaviors and Controls

Typically, when IT roles are revoked in a certification, LCM request, or policy violation remediation, either as part of the revocation of an associated business role or independently, the corresponding entitlements are also revoked from the identity unless those same entitlements are required by another role the identity holds.  In version 6.0, IdentityIQ began tracking whether entitlements were explicitly marked as “assigned” in their association to users and treating those assigned entitlements differently.  Specifically, assigned entitlements were not revoked when a role containing them was revoked.  Because this caused confusion with some customers, version 6.4 added configuration options around this behavior.

****NOTE****: Entitlements are marked as assigned by IdentityIQ when they are directly requested in Lifecycle Manager (not through a role) or when they are approved in a certification which has specified the option to update entitlement assignments.  Some customers may also use their own custom processes or a batch update process to explicitly mark entitlements as assigned for identities in their installation.

The chart below describes the role revocation behaviors according to product versions.

|  |  |
| --- | --- |
| ****IdentityIQ Version**** | ****Role Entitlement Revocation Behavior**** |
| 5.5 | Entitlements included under a role definition are auto-revoked when the role is revoked.  The entitlement assignment concept does not exist prior to version 6.0. |
| 6.0 - 6.3 | Entitlements are marked as assigned when directly requested (not through a role) and optionally upon certification approval (based on certification configuration).  Assigned entitlements are not auto-revoked when a role encompassing them is revoked.  Non-assigned entitlements are auto-revoked when a role encompassing them is revoked. |
| 6.4+ | Entitlements are marked as assigned when directly requested (not through a role) and optionally upon certification approval.  By default, any entitlement (assigned or not) will be auto-revoked with the role revocation, but assigned entitlements can be retained when a role encompassing them is revoked, based on system configuration settings. |

The system configuration options which can make the system retain assigned entitlements in version 6.4 are found on the gear menu -> ****Global Settings**** -> ****IdentityIQ Configuration**** -> ****Roles**** page and are called

* ****Retain assigned entitlements when detected roles are removed**** and
* ****Retain assigned entitlements when assigned roles are removed****

Most customers will choose to accept the default behavior and not use these options, but they are provided to offer that flexibility where it is needed.  The type of role being explicitly revoked through LCM or a certification determines which of these options applies, though the two options would usually be enabled or disabled together.

For example, if Business role A (which requires IT role X) is revoked, IT role X’s entitlements would be retained only if ****Retain assigned entitlements when assigned roles are removed**** is set.  If IT role Y is directly revoked (it appears outside a business role either because it is a permitted role which can be processed independently in LCM or because it is a detected role with no corresponding business role assignment), its underlying entitlements would only be retained if ****Retain assigned entitlements when detected roles are removed**** is set.

#### Identity Refresh Role Revocation

An identity refresh task with the ****Refresh assigned, detected roles and promote additional entitlements**** option selected can deassign business roles when the user no longer meets the assignment rules’ criteria (e.g. they no longer belong to the relevant department or hold the corresponding job title).  The ****Retain assigned entitlements…**** options discussed above do not apply to an identity refresh task; they are only used for entitlement retention when a role is revoked based on a human-interaction request.  An option called ****Disable deprovisioning of deassigned roles**** is available on identity refresh tasks which will remove the business role without removing any of the underlying entitlements – whether those entitlements are marked as assigned or not.  As with the two Retain assigned entitlements... options, this option is seldom used.

# Role Lifecycle Management

In addition to the role engineering capabilities provided by the Role Modeler and role mining activities, IdentityIQ includes end-to-end role lifecycle management capabilities to help organizations manage roles over their entire lifecycle, from creation to retirement.  These include automated role approvals, role analytics, role certifications (role membership and contents), and role quality metrics.  IdentityIQ’s support of future-dated activation/deactivation and assignment/deassignment of roles, along with its role versioning capabilities, also aids in managing role lifecycles.

Role approvals and role analytics provide governance around roles; they occur, either automatically or in response to a user request, as roles are being created and modified.  Role certifications and role quality metrics provide additional resources for monitoring and managing roles over time as business and IT environments change.

## Role Approvals

The role approval process ensures that the role owner (and any other specified Identities) is aware of and approves any changes to the roles for which they are responsible.  By default, newly created or changed roles go through an approval process managed through an approval workflow that routes the new or modified role to the role owner for approval.  If the person who created or changed the role is also the role owner, this approval step is bypassed.  The default workflow can be customized to add or alter approval steps to meet each organization’s business requirements.

## Role Analytics

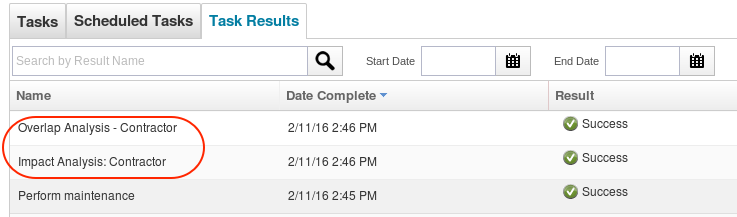
Role analytics provide statistical analyses of roles and detectable patterns within and between them.  The statistics’ supporting detail is also included and can be used by the organization to evaluate the data in a meaningful way.

### Role Impact Analysis

Role uniqueness, as well as the role membership impact of a role creation or change, can be measured through a role impact analysis. An impact analysis can be run in one of two places in the IdentityIQ UI:

* ****Setup**** -> ****Roles**** -> select role -> ****Edit**** -> ****Submit with Impact Analysis****
* ****Setup**** -> ****Tasks**** -> ****Role Overlap Analysis****

Either way they are generated, the analysis results can be viewed from the Task Results window (****Setup**** -> ****Tasks**** -> ****Task Results****). If run from the task window, the task name will be ****Overlap Analysis – [Role Name]****, whereas the task name when run from the Role window is ****Impact Analysis: [Role Name]****.



In both cases, the analysis is run for one role at a time.  Two distinct impacts are considered and reported in the details of the task results: role membership changes and role overlap.

#### Role Membership Changes

Changes to role memberships are reflected in the ****Impact Analysis Summary**** section of the Impact or Overlap Analysis task results, with the details of the affected roles shown below the summary.  Membership gains and losses for the selected role are shown, as are gains and losses incurred by other roles as a result of the selected role’s creation or change.

****Note****: Gains and losses only apply to detected roles, not role assignments.

#### Role Overlap

In the Overlap analysis, the selected role is compared to all other roles in the system based on two key metrics:

* ****Assignment****: the attribute and permission profiles by which an IT role is detected for an Identity or the assignment rule (selector) for assigning a business role to an Identity
* ****Provisioning****: the entitlements within the provisioning plan or profile for the role and any required roles associated with it

Two percentages are calculated for each metric: one based only on each role by itself (Local) and one based on each role’s inheritance (Hierarchical).  In other words, the Hierarchical percentages are calculated based on the percentage overlap of the metric for all roles from which the examined roles inherit as well as the roles themselves. The Local and Hierarchical analyses parallel the Direct and Indirect association concepts discussed with respect to Role Statistics.

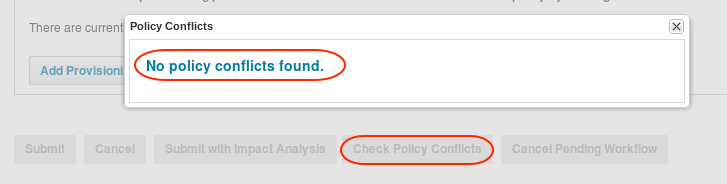
The analysis summary contains a list of all roles with which the role has overlapping components. The analysis scores for each role are calculated as percentages: the number of matching components in a category as a percentage of the total number of comparison points in that category.

In many cases, it is appropriate for some roles to overlap with others, so these analysis results do not necessarily indicate any problems.  The analysis simply serves as another tool for assessing the defined set of roles to minimize redundancy and help control role proliferation.

### Policy Validation

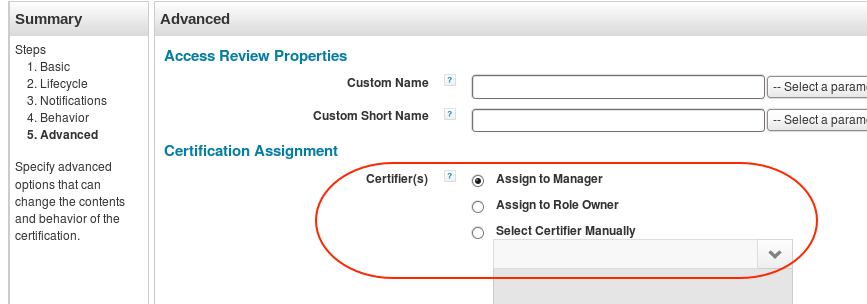
The ****Impact Analysis**** section of the analysis results also includes a statistic on policy violations detected for the selected role.  This statistic is calculated by evaluating the role against the defined Policies in the system and determining if it will cause violations of any of those Policies. For example, if business role “AP – Accountant” required two IT roles “AP – Entry” and “AP – Approval” that are in conflict according to a configured Policy, the policy validation process on that business role will detect and report this violation.

The policy validation process can be requested for a role independent from an impact analysis as well. At the bottom of the Role Editor window, click Check Policy Conflicts.  Any detected policy conflicts are immediately reported to the user.



## Role Membership Certification

The Role Membership Certification is another useful tool in role lifecycle management. This certification focuses on the set of Identities to which one or more selected roles is assigned.  Certification responsibility can be assigned to each Identity’s Manager, to the Role Owner, or to a specifically selected certifier – whoever is best equipped to determine whether the roles’ members should hold the roles or not.



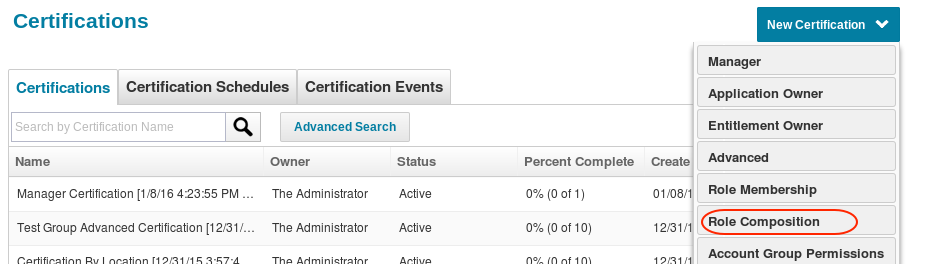
Often, this certification type is used during the role creation process to validate the sets of identities grouped together under a mined or manually created business role even before that role is connected to any required or permitted IT roles.  This helps validate the role structure and any automatic assignment rules created for the roles before it has any impact on application entitlement provisioning.

## Certification of Role Composition

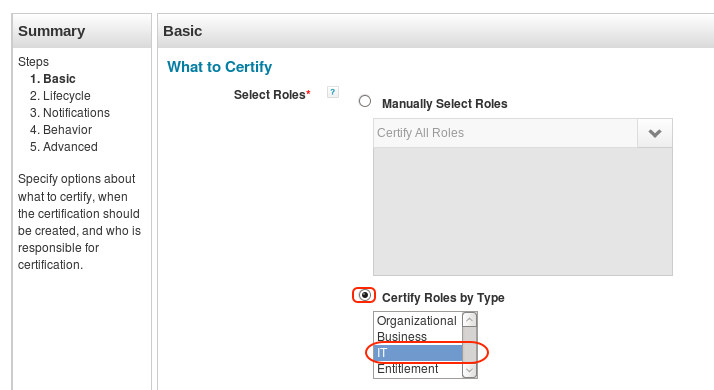
To ensure that roles are appropriately defined, organizations can and should certify the makeup of roles themselves.  This is separate from and equally as important as certification of role assignments.  Defined roles that are missing critical components or that include invalid entitlements for the role can be at best inefficient and at worst a source of business risk.

The Role Composition Certification allows the organization to collect this role information and present it to someone who understands what is appropriate for the role, who can evaluate the role’s makeup, and who can make adjustments as needed.

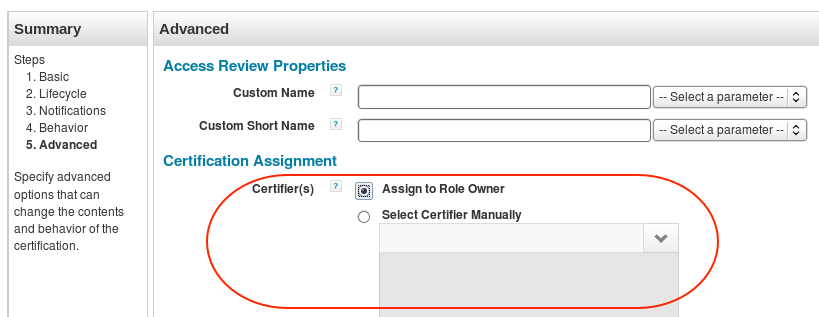
To run a Role Composition Certification, select ****Setup**** -> ****Certifications****.  Then select ****Role Composition**** from the ****New Certification**** list.



On the ****Basic**** page, select the roles to certify and whether to include each role’s hierarchy in the certification.



On the ****Advanced**** page, specify the ****Certifier(s)****.  The default is for each role to be certified by its owner, but the entire set in a given certification can alternatively be assigned to one selected certifier. Select a certifier who is knowledgeable about what the role composition should be.



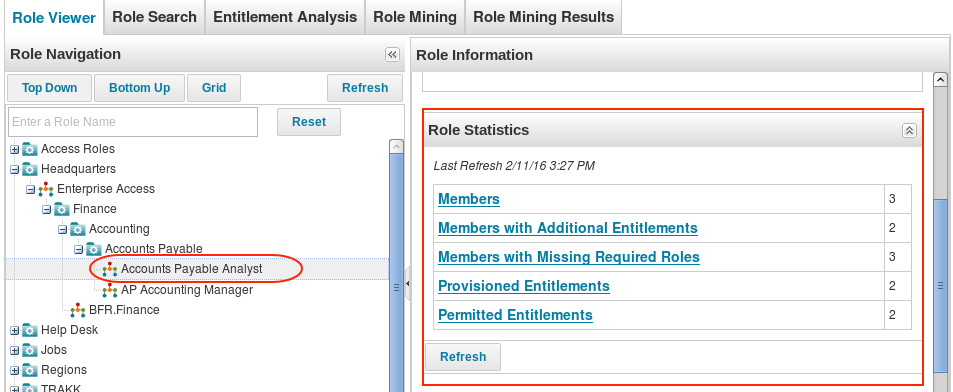
Alter any other certification parameters on any of the pages as desired and schedule the certification.

## Role Quality Analysis Tools

The IdentityIQ Role Modeler provides several tools for analyzing the role structure to identify overlapping roles, missing entitlements for Identities assigned to roles, Identities who may be missing assigned roles based on their detected role status, and so on.  These tools can help the administrator make adjustments to the role structure to improve its usefulness to the organization.

### Role Statistics

Statistics recorded on each IT and business role can be used to judge data quality on a per-role basis.  These statistics can be seen on the Role Management window (****Setup**** -> ****Roles****) in the ****Role Statistics**** section of the ****Role Information**** pane.



Before role statistics can be generated, role metadata must be gathered for each identity; this data is required for the role statistics calculations.  To generate that data, run an Identity Refresh task with the ****Refresh role metadata for each identity**** option selected.  Then, to generate or regenerate the statistics for a single role, click ****Refresh**** below the ****Role Statistics**** in that role’s ****Role Information**** pane.  To generate or regenerate statistics for all business and IT roles, run the ****Refresh Role Scorecard**** task.

#### Direct vs. Indirect Role Association

Roles can be associated to Identities either directly or indirectly.  A business role that is “directly” associated with an Identity is one that is explicitly assigned to the Identity.  If the Identity is assigned to a role that inherits from another business role, it is considered to be “indirectly” associated to the parent role.  Similarly, an IT role is “directly” associated with an Identity when the role itself is detected for the Identity.  It is “indirectly” associated when a role that inherits from it is detected for the Identity.  All Role Statistics look at both direct and indirect associations for a business role, so all Identities that are assigned to or detected for the role or any of its “child” roles are included in the role’s statistical counts.

#### Business Role Statistics

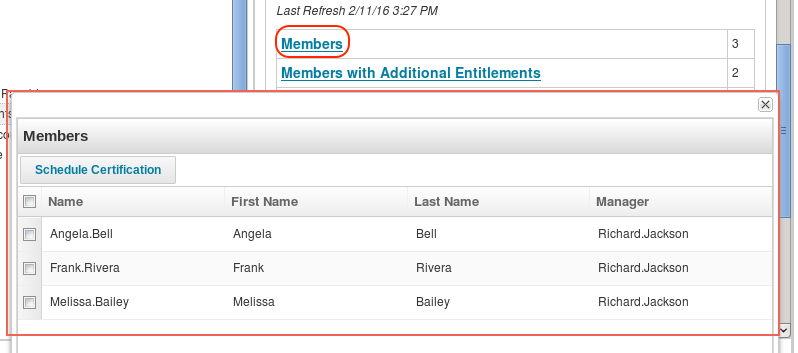
For business roles, these 5 categories are calculated and reported:

* ****Members****: Number of Identities assigned to this role, either directly or indirectly
* ****Members with Additional Entitlements****: number of Identities assigned to this role (directly or indirectly) who have non-role-based entitlements
* ****Members with Missing Required Roles****: number of Identities assigned to this role (directly or indirectly) who are missing some of the role’s required IT roles
* ****Provisioned Entitlements****: Number of entitlements that will be provisioned for an Identity when this role is assigned (total count of entitlements associated with the required IT roles for this business role)
* ****Permitted Entitlements****: Number of entitlements that will be provisioned by roles required or permitted by this role (total count of entitlements associated with the required and permitted IT roles for this business role)

In most cases, the meaning of these statistics is subjective and must be evaluated by each organization.  For example, one role may appropriately have hundreds or thousands of Identities assigned to it while another might be appropriate for only a handful of employees, so the “appropriate” member count may vary greatly from one role to another.  Additionally, if the organization is managing all entitlements through roles (which is rare), the Members with Additional Entitlements value should be zero in all cases because Identities should not have any entitlements outside of their assigned roles, but if only some access is managed through roles, the Members with Additional Entitlements information may not be very meaningful to the organization.

The ****Members with Missing Required Roles**** statistic is the exception to this subjectivity. A non-zero value for this statistic is always an indication of a likely problem because any identity assigned a role should have all of the entitlements required for it.

Each statistical category name is a link to the supporting data for its value.  Click the ****Members****, ****Members with Additional Entitlements****, or ****Members with Missing Required Roles**** link to view a list of all Identities in that category.  Click the ****Provisioned Entitlements**** or ****Permitted Entitlements**** link to view the list of entitlements in that group for the role.

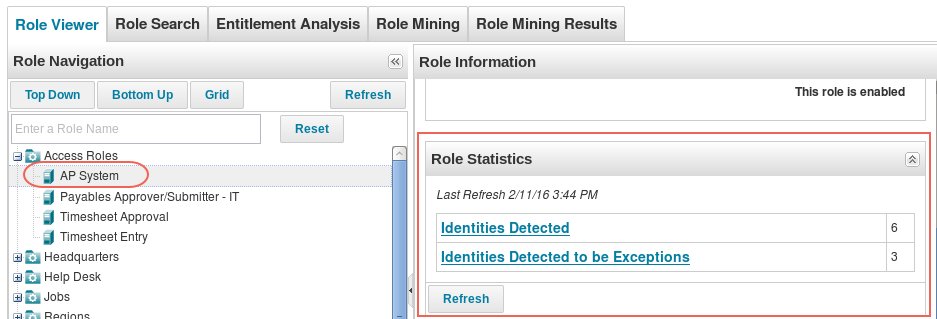


#### IT Role Statistics

For IT roles, the statistics that are reported are:

* ****Identities Detected****: Number of Identities for whom this IT role has been detected (Identity has all entitlements of this role)
* ****Identities Detected to be Exceptions****: Identities who have all the entitlements of this role (and therefore have the role detected) but are not assigned any business role that requires or permits it

The quality assessment of role data based on these statistics is again subjective. However, these statistics, and the supporting list of Identities that can be viewed by clicking the category name link, can be helpful in analyzing roles and determine if and when adjustments to the defined role structure should be made.



### Role Reports

Several role-focused reports are available out of the box to help with role analysis. They are:

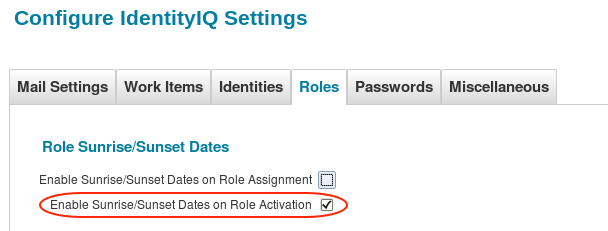
* ****Role Composition Access Review Report****: shows detailed role composition certification information
* ****Role Membership Access Review Report****: shows detailed role membership certification information
* ****Access Request Status Report****: lists Requestor, Requested For, Request Date, Operation, Role, Rejected By, Status, Completion Date, and Comments
* ****Role Archive Report****: shows role information in Archive Format (detailed view)
* ****Role Change History Report****: lists Name, Type, Version, Date of Change, Approver, and Status
  + ****NOTE****: This report only contains results if doArchive is set to “true” in the active role approval workflow (role versioning is built into the out of the box Role Modeler – Owner Approval and Role Modeler - Impact Analysis workflows if activated with this workflow variable).
* ****Role Profiles Composition Report****: lists Role Name, Profile Filter(s), and Application(s) to which this role grants access
* ****Role Detail Report****: lists Role Name, Owner, Role Type, and Application(s) to which this role grants access
* ****Role Members Report****: lists Role Name, Identity, First and Last Name

These reports are additional resources for analyzing the installation’s defined role structure.

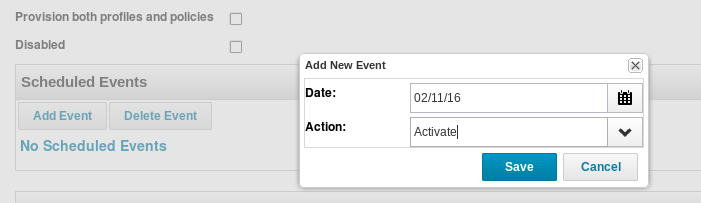
## Future-Dated Role Activation and Deactivation

IdentityIQ supports specifying future-dated activation and deactivation events for roles, commonly referred to as “sunrise” and “sunset” dates. These provide additional options for managing role lifecycles.

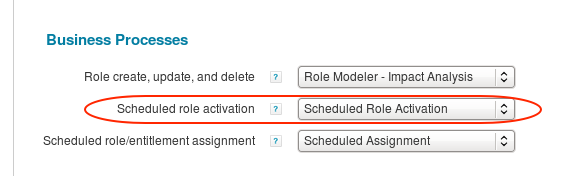
This feature must be explicitly turned on through the system configuration pages: navigate to gear menu -> ****Global Settings**** -> ****IdentityIQ Configuration**** -> ****Roles**** and select the ****Enable Sunrise/Sunset Dates on Role Activation**** option.



Each role then offers the option of specifying events for activation and deactivation in the Role Editor.  To schedule a role for future activation, first mark the role as Disabled (some role modeling activities automatically create roles in this disabled state).  Then choose ****Add Event**** in the ****Scheduled Events**** section of the ****Role Editor**** page.  Specify the desired activation ****Date**** and choose ****Action****: ****Activate****.  To schedule a role for future deactivation, choose ****Action****: ****Deactivate**** when creating an event.

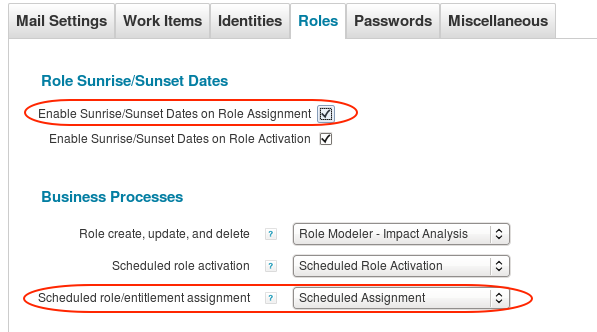


The system automatically processes the activation/deactivation request on the specified date using a workflow.  The default workflow run is ****Scheduled Role Activation****, though the system can be pointed to a different workflow through the gear menu -> ****Global Settings**** -> ****IdentityIQ Configuration**** -> ****Roles**** page by selecting a different Scheduled role activation business process.

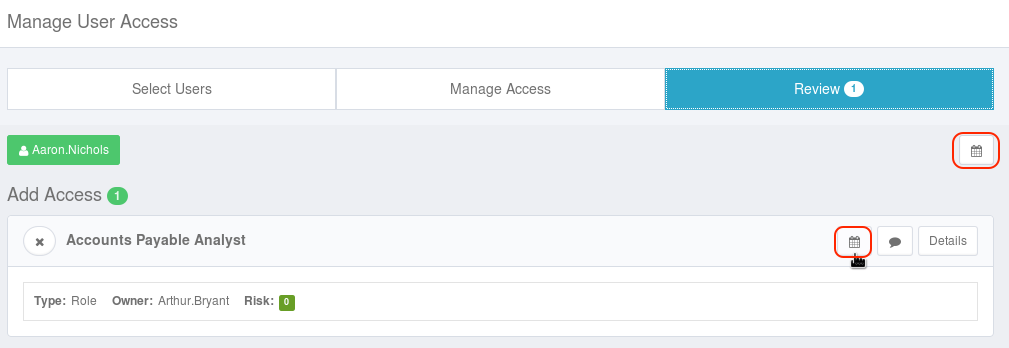


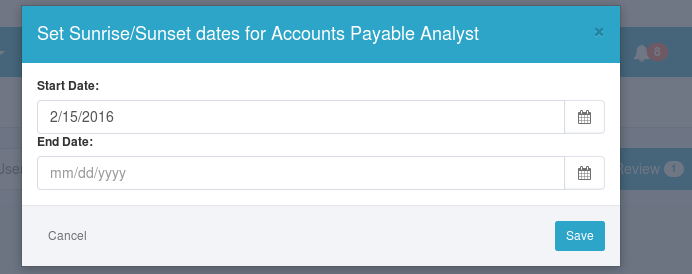
### Future-Dated Role Assignment/Deassignment

Role assignments (and deassignments) can also be scheduled for a future date.  This feature must be turned on with the ****Enable Sunrise/Sunset Dates on Role Assignment**** option, and the workflow to control the assignment/deassignment process can be specified as the ****Scheduled role/entitlement assignment**** business process in the ****Roles**** system configuration page (default workflow is ****Scheduled Assignment****).



For each role assignment made through Lifecycle Manager, select an activation and/or deactivation date for the whole cart or for each line item on the ****Review**** page.  The system automatically processes the assignment/deassignment request on the specified date(s) using the workflow selected for managing scheduled role/entitlement assignment (above).

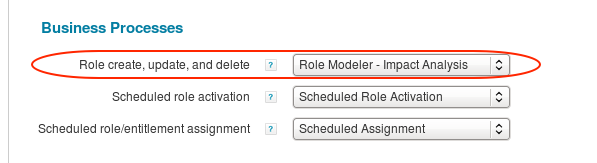




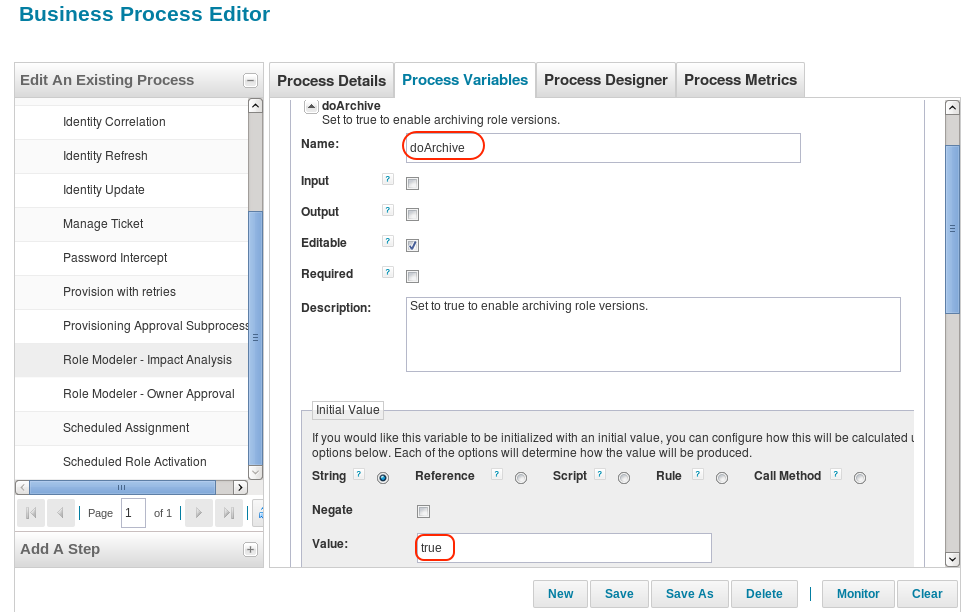
## Role Versioning

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 workflows 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.

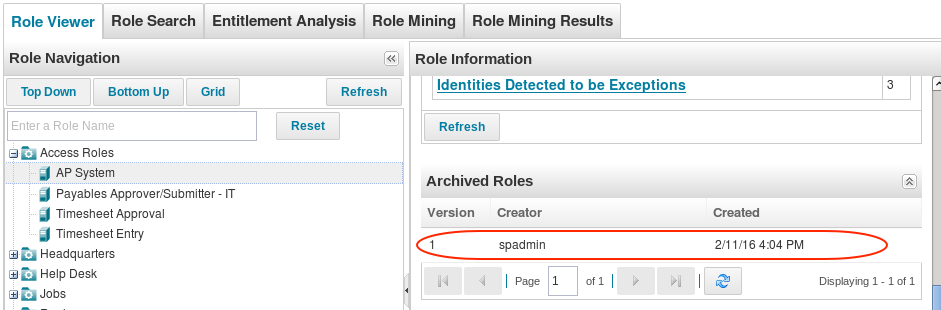
When role changes occur, a workflow is launched to process the changes; this may perform approval processes, impact analyses, etc.  The workflow that is launched is specified on the gear menu -> ****Global Settings****-> ****IdentityIQ Configuration****-> ****Roles****page as the ****Role create, update, and delete****business process.



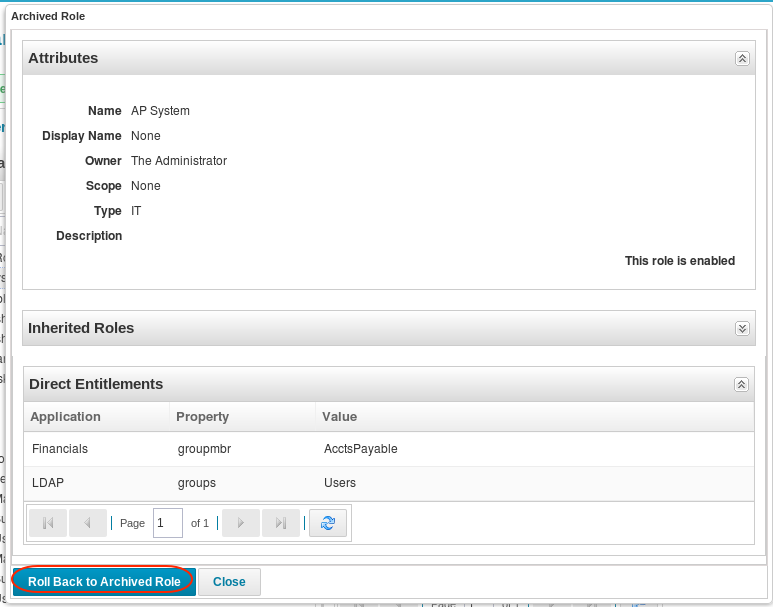
In that workflow, set the ****doArchive**** variable to true through the Business Process Editor (****Setup**** -> ****Business Process**** -> select business process) or workflow XML.



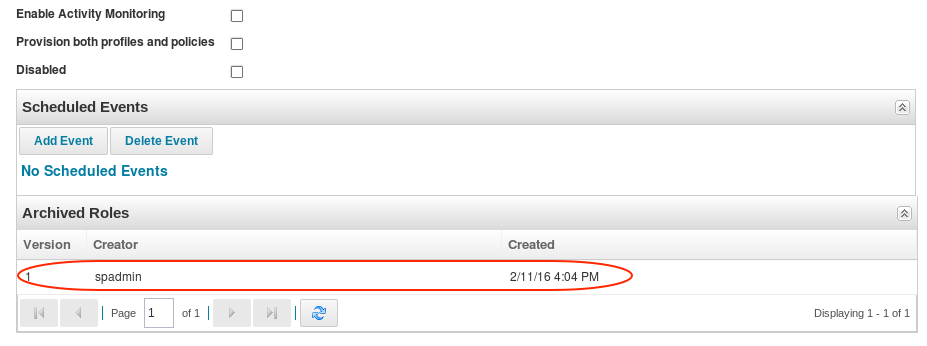
Any time a role is changed (after any approval processes have finished and the change has been fully activated), an archive version of its previous state is saved.  To view the set of previous states for a role, click the role name in the Role Viewer Navigation list (****Setup**** -> ****Roles**** -> ****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 available from the Role Editor page as well (visible by clicking ****Edit Role**** from the Role Viewer page).  Find the ****Archived Roles**** section, expand it to view the archived versions, click one to see its details, click ****Roll Back to Archived Role****, and ****Submit**** it to restore that version.



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 (with the ****Refresh assigned, detected roles and promote additional entitlements**** option selected) runs to update those associations unless the role change workflow 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.