

SailPoint IIQ-6.4

Roles in IdentityIQ

Roles in IdentityIQ

Role: A role is a collection of entitlements or other roles that enables an identity to access the resources and to perform certain operations within an organization.

Need for Role's in IdentityIQ:

- 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.
- It helps enterprises line up low-level IT privileges with their corporate structure and business operations by grouping individual entitlements into higher-level business functions.
- Translate entitlement data into terms that can be most understood by business managers and other employees when they certify and examine the data.

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

1. Organizational Role.
2. Business Role.
3. IT Role.
4. Entitlement Role.

We will discuss the various possible usages of the role structures in their default configuration as shown below.

1. **Organization Role:** Designed for organizing the role hierarchy in IdentityIQ UI. They do not perform any function other than creating a nesting structure in the Role Modeler.

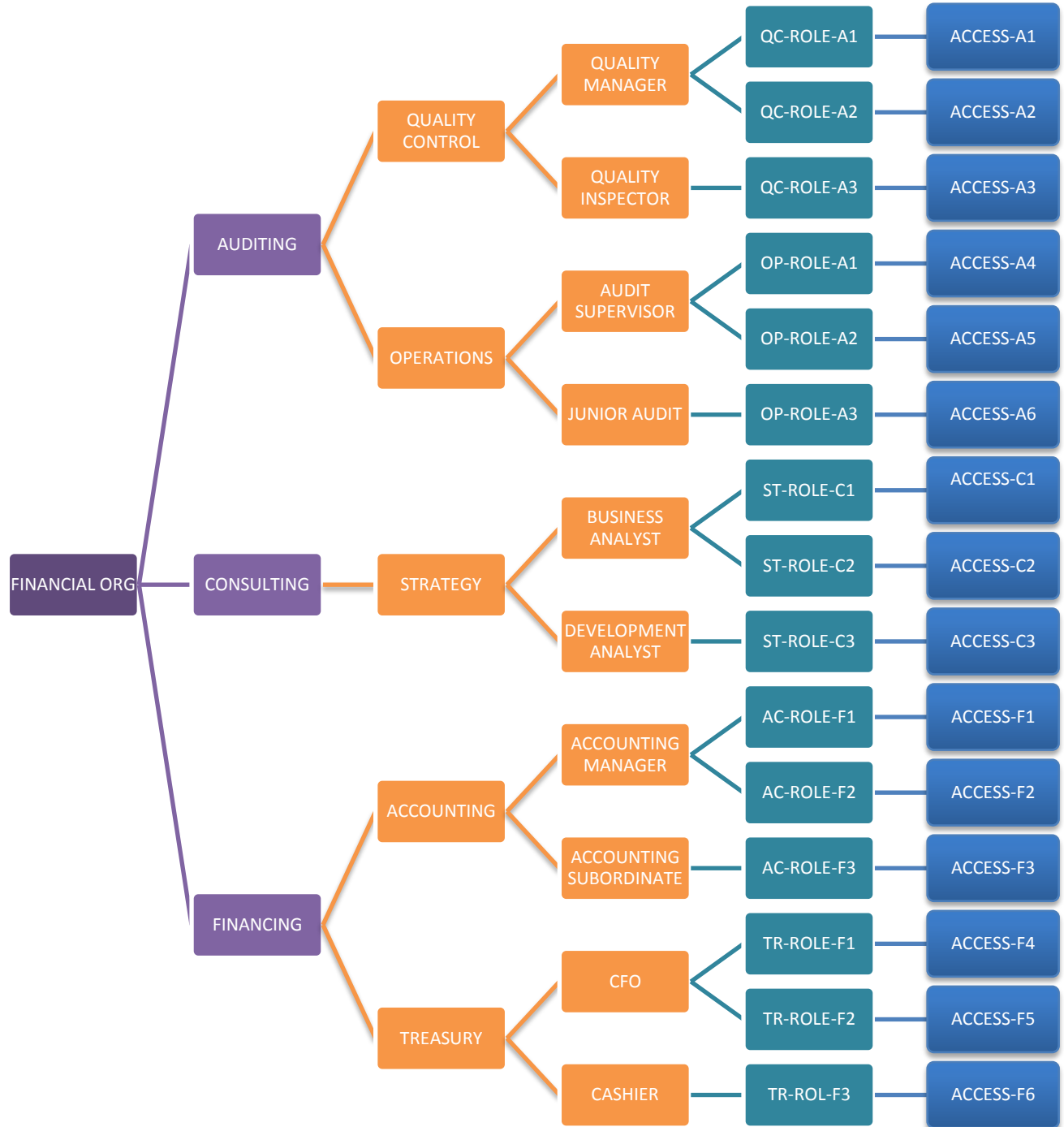
Possible Organizational structures could include:

- A hierarchy matching the corporate org structure for organizing business roles into easily managed groupings.
- A set of container roles for holding IT roles collections based on commonalities
- A set of container roles grouping other roles by application
- A set of container roles grouping other roles alphabetically

Organization Role creates a familiar and easily navigable framework for managing the business role model. This makes it easier to identify and create the component business roles, and it facilitates finding and managing roles as changes occur in the future.

Roles in IdentityIQ

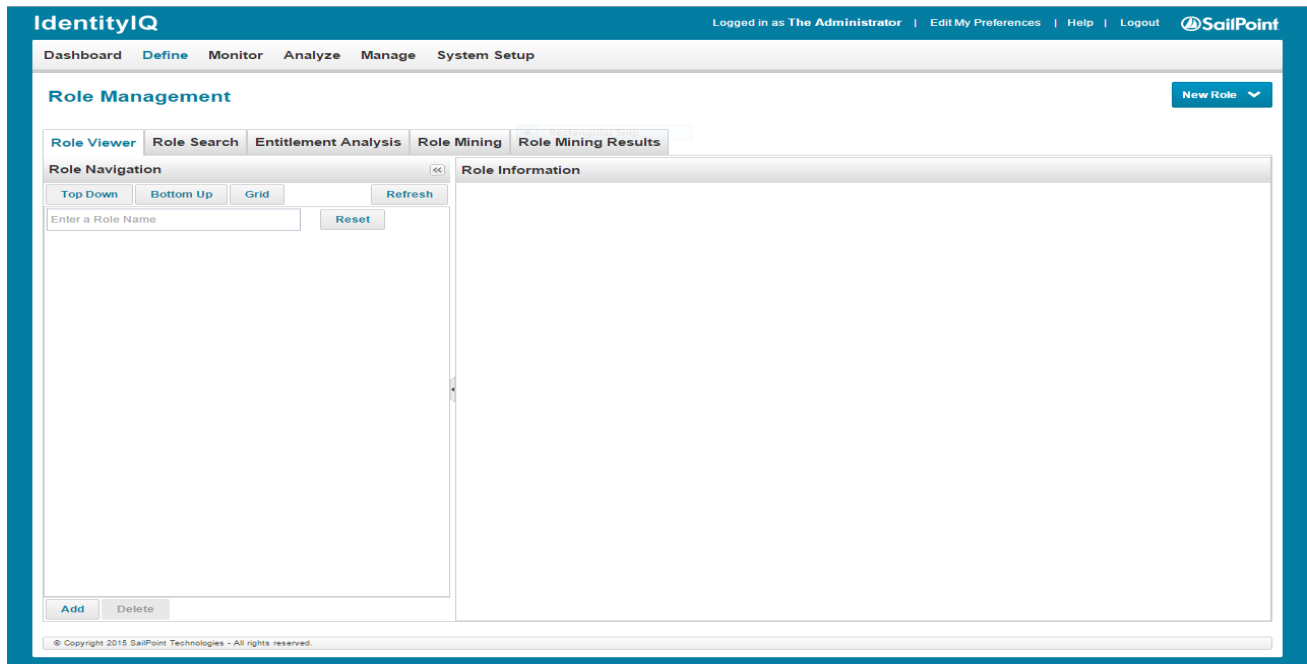
2. Example Model:



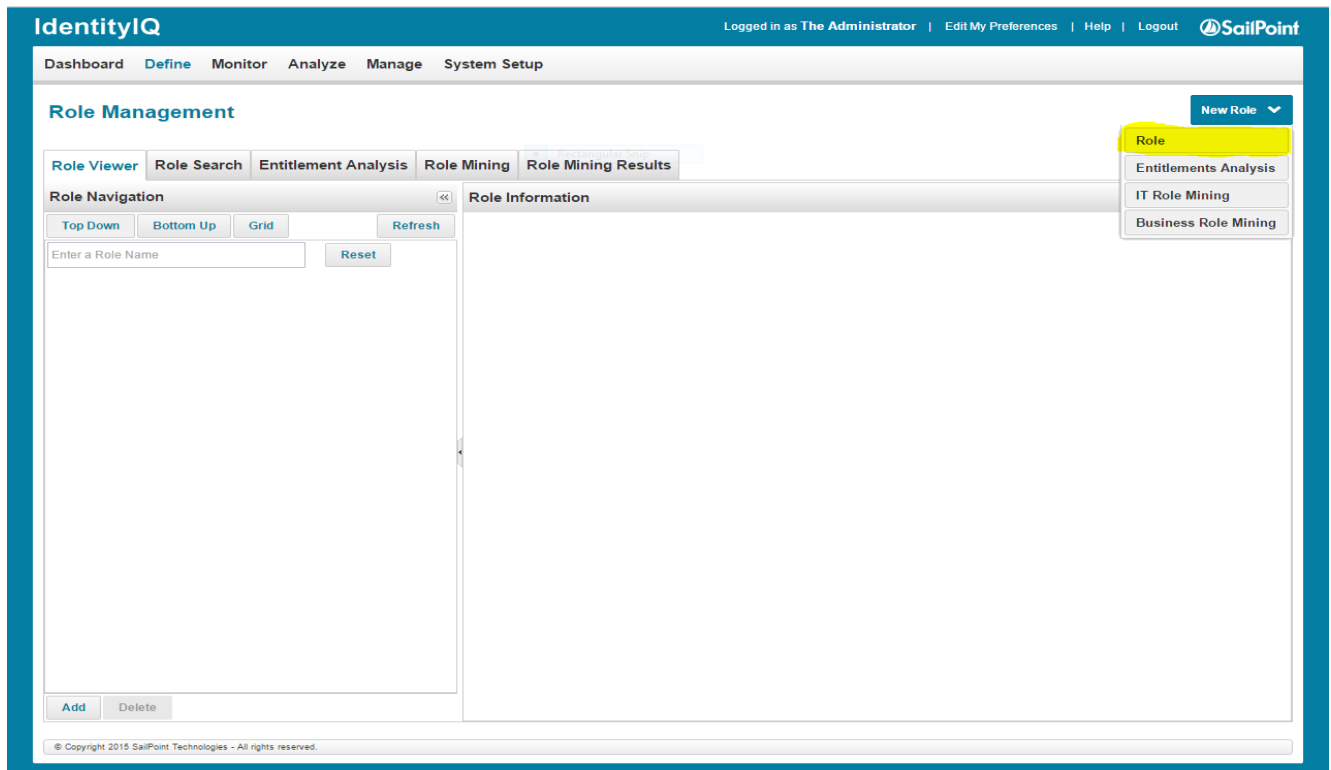
Roles in IdentityIQ

Creating an Organization Role:

STEP-1: GO TO Define Roles New Role as shown below



STEP-2: Click on **New Role** and select **Role**, the following screen is displayed. Enter the required fields and click on **Submit**.



Roles in IdentityIQ

Required Fields on Role Editor Page:

1. **Name:** Name of the IT Role.
2. **Display Name:** Display Name for the IT Role.
3. **Type:** Select type as **Organizational** from the drop down menu.
4. **Owner:** select the Owner for the IT Role.
5. **Description:** Description for the IT Role.
6. **Enable Activity Monitoring:** To enable/disable the Activity Monitoring.
7. **Disabled:** Enable/Disable the Role.
8. **Modify Inheritance:** To inherit any other roles, click on **modify Inheritance**.

STEP-3: Select Type as **Organizational** as shown below.

The screenshot displays the IdentityIQ Role Editor interface. At the top, the user is logged in as 'The Administrator'. The navigation bar includes 'Dashboard', 'Define', 'Monitor', 'Analyze', 'Manage', and 'System Setup'. The 'Role Editor' section is active, showing a form for editing a role named 'FINANCIAL ORG'. The 'Name' and 'Display Name' fields are both set to 'FINANCIAL ORG'. The 'Type' dropdown menu is set to 'Organizational'. The 'Owner' is set to 'The Administrator'. The 'Description' field contains the text 'Financial Organization'. Below the description, there are three checkboxes: 'Enable Activity Monitoring', 'Provision both profiles and policies', and 'Disabled', all of which are currently unchecked. The 'Inherited Roles' section shows a 'Modify Inheritance' button and a message stating 'This role does not inherit any other roles.' The 'Provisioning Policy' section shows a message stating 'There are currently no provisioning policies defined.' and buttons for 'Add Provisioning Policy' and 'Delete Provisioning Policy'. At the bottom, there are buttons for 'Submit', 'Cancel', 'Submit with Impact Analysis', and 'Check Policy Conflicts'.

IdentityIQ

Logged in as The Administrator | Edit My Preferences | Help | Logout | SailPoint

Dashboard Define Monitor Analyze Manage System Setup

Role Editor

*Indicates a required field.

Name * FINANCIAL ORG Rectangular Snip

Display Name FINANCIAL ORG

Type * Organizational ▼

Owner * The Administrator ▼

Description

B *I* U | English (United States) ▼

Financial Organization

22 of 1024 characters (including markup)

Enable Activity Monitoring ☐

Provision both profiles and policies ☐

Disabled ☐

Inherited Roles

Modify Inheritance

This role does not inherit any other roles.

Provisioning Policy

Below is a list of provisioning policies associated with this role. You can add a new policy by clicking on the 'Add Provisioning Policy' button below or edit an existing one by clicking on it in the list.

There are currently no provisioning policies defined.

Add Provisioning Policy Delete Provisioning Policy

Submit Cancel Submit with Impact Analysis Check Policy Conflicts

Roles in IdentityIQ

STEP-4: The following page is displayed on selecting the Modify Inheritance as shown below.

The screenshot shows the IdentityIQ Role Editor interface. The main form has fields for Name (FINANCIAL ORG), Display Name (FINANCIAL ORG), Type (Organizational), Owner (The Administrator), and Description. A 'Modify Inheritance' dialog is open, showing a table with columns Name, Type, and Description. The dialog also has a 'Remove Selected' button and a 'No data to display' message. Below the dialog, there are buttons for 'Save' and 'Cancel'. The background form also has a 'Provisioning Policy' section with a message: 'Below is a list of provisioning policies associated with this role. You can add a new policy by clicking on the 'Add Provisioning Policy' button below or edit an existing one by clicking on it in the list. There are currently no provisioning policies defined.'

STEP-5: Add the Roles you want to inherit into this Organization Role and save it. And the created roles will be viewed under the **View Roles** tab

The screenshot shows the IdentityIQ Role Management interface. The 'Role Information' tab is selected, displaying details for the role 'FINANCIAL ORG'. The details include Name, Display Name, Owner, Scope, Type, and Description. A 'Refresh' button is visible. The 'Role Statistics' section is also shown. The 'Role Navigation' section on the left has a search bar and a 'Reset' button. A message at the top states: 'The role named 'FINANCIAL ORG' was successfully saved.'

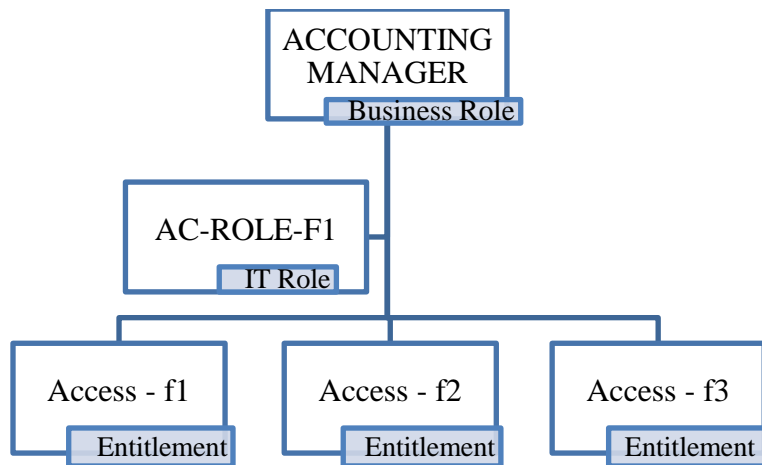
Roles in IdentityIQ

2. **Business Role:** Identifying job functions or titles or other attributes by which users can be grouped together into a Business Role.

For example, within the Financing Organization, there might be an Accountant, 3 Cashiers, and some people under Treasury. This would require the creation of business roles:

- **Accounting**
- **Treasury**

Example:



Creation of a Business Role:

STEP-1: GO TO Define Roles, Click on **New Role** and select **Role** the following screen is displayed as shown.

IdentityIQ

Logged in as The Administrator | Edit My Preferences | Help | Logout | SailPoint

Dashboard Define Monitor Analyze Manage System Setup

Role Management

Role Viewer Role Search Entitlement Analysis Role Mining Role Mining Results

Role Navigation

Top Down Bottom Up Grid Refresh

Enter a Role Name

AUDITING CONSULTING FINANCIAL ORG FINANCING

Reset

Role Information

Attributes

Name FINANCING

Display Name FINANCING

Owner The Administrator

Scope None

Type Organizational

Description Financing Organizational Unit

This role is enabled

Role Statistics

Refresh

Add Delete Edit Role

© Copyright 2015 SailPoint Technologies - All rights reserved.

Roles in IdentityIQ

STEP-2: Select Type as **Business**, the following screen is displayed. Enter the required fields and click on **Submit**.

The screenshot shows the IdentityIQ Role Editor interface. The top navigation bar includes 'Dashboard', 'Define', 'Monitor', 'Analyze', 'Manage', and 'System Setup'. The user is logged in as 'The Administrator'. The 'Role Editor' section contains the following fields and options:

- Name:** ACCOUNTING
- Display Name:** ACCOUNTING
- Type:** Business (selected from a dropdown menu)
- Owner:** The Administrator (selected from a dropdown menu)
- Description:** Accounting Business Role - Financing Organization (with a character count of 49 of 1024 characters)
- Enable Activity Monitoring:** ☐
- Provision both profiles and policies:** ☐
- Disabled:** ☐
- Assignment Rule:** None (selected from a radio button group)
- Required Roles:** No Required Roles (with a 'Modify Required Roles' button)
- Permitted Roles:** (empty section with a 'Modify Permitted Roles' button)

Required Fields on Role Editor Page:

1. **Name:** Name of the Business Role.
2. **Display Name:** Display Name for the Business Role.
3. **Type:** Select type as **Business** from the drop down menu.
4. **Owner:** select the Owner for the Business Role.
5. **Description:** Description for the Business Role.
6. **Enable Activity Monitoring:** To enable/disable the Activity Monitoring.
7. **Disabled:** Enable/Disable the Role.
8. **Inherited Roles:** To inherit any other roles, click on **modify Inheritance**.
9. **Entitlements:** Select the Entitlements you want to group them as a role.
10. **Required Roles:** To add roles into this, click on **Modify Required Roles**.
11. **Permitted Roles:** To add roles into this, click on **Modify Permitted Roles**.

Required Roles: Required Roles are the IT roles that an Identity must have when they are associated with that business role.

Add the appropriate IT Roles for the Required Roles and click on **Save**.

Roles in IdentityIQ

IdentityIQ

Logged in as The Administrator | Edit My Preferences | Help | Logout

SailPoint

Dashboard

Define

Monitor

Analyze

Manage

System Setup

Role Editor

*Indicates a required field.

Name *

ACCOUNTING

Display Name

ACCOUNTING

Type *

Business

Owner *

The Administrator

Description

B

I

U

L

I

I

I

English (United States)

Accounting Business Role - Financing Organization

49 of 1024 characters (including markup)

Enable Activity Monitoring

☐

Provision both profiles and policies

☐

Disabled

☐

Assignment Rule

None

Match List

Filter

Script

Rule

Population

Required Roles

Modify Required Roles

No Required Roles

Permitted Roles: Permitted Roles are the ones that the Identity can have but is not required to have when assigned that business role.

Add the appropriate IT Roles for the Permitted Roles and click on **Save**.

IdentityIQ

Logged in as The Administrator | Edit My Preferences | Help | Logout

SailPoint

Dashboard

Define

Monitor

Analyze

Manage

System Setup

Role Editor

*Indicates a required field.

Name *

ACCOUNTING

Display Name

ACCOUNTING

Type *

Business

Owner *

The Administrator

Description

B

I

U

L

I

I

I

English (United States)

Accounting Business Role - Financing Organization

49 of 1024 characters (including markup)

Enable Activity Monitoring

☐

Provision both profiles and policies

☐

Disabled

☐

Assignment Rule

None

Match List

Filter

Script

Rule

Population

Required Roles

Modify Required Roles

No Required Roles

Permitted Roles

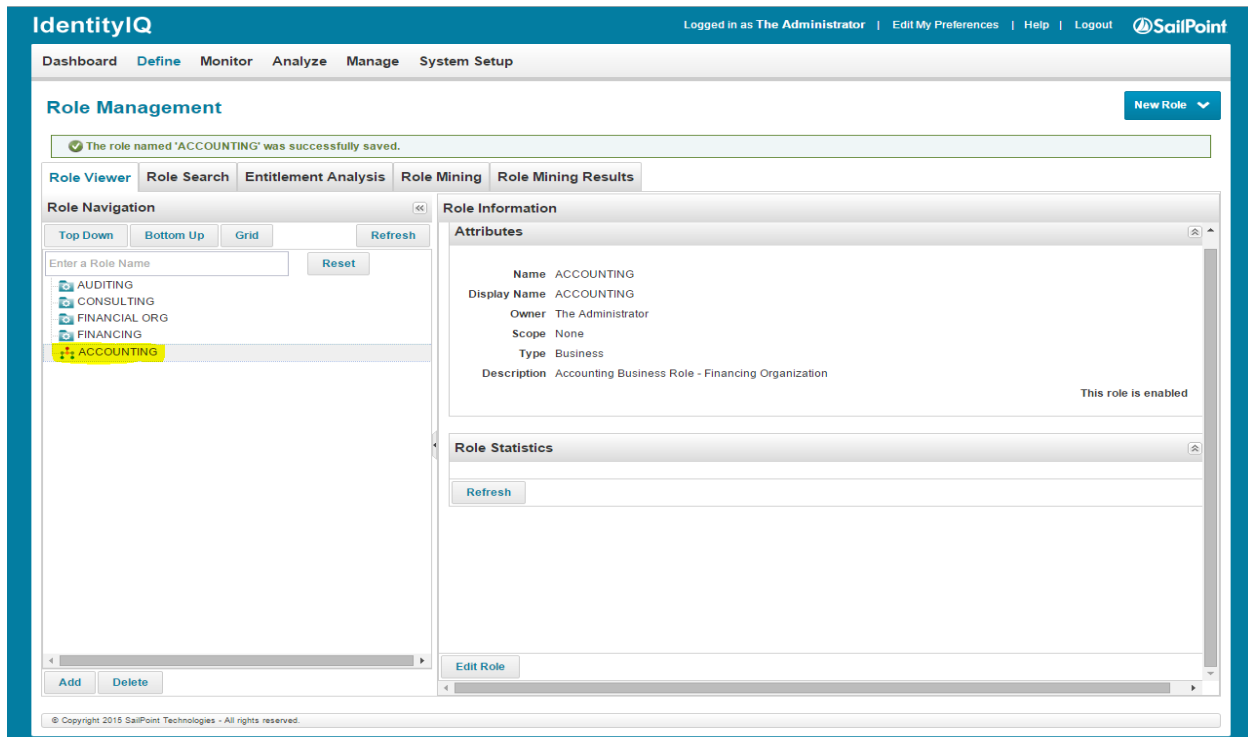
Modify Permitted Roles

No Permitted Roles

Inherited Roles

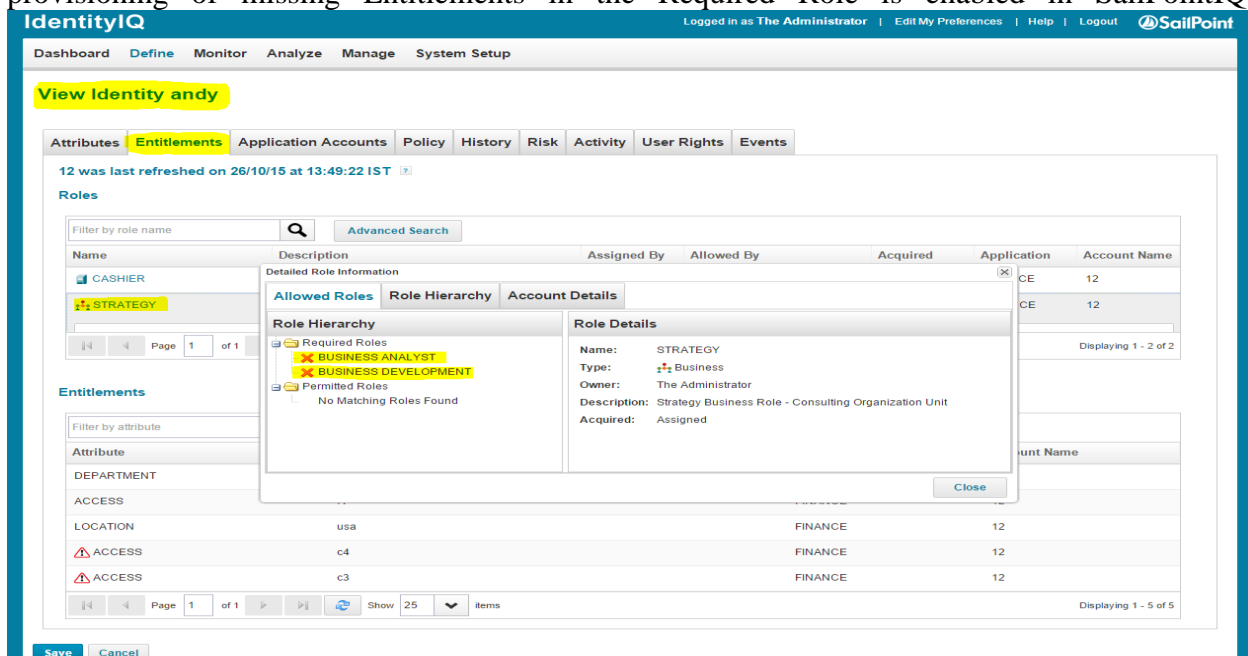
Roles in IdentityIQ

STEP-3: The created Business Roles are listed down under Role Viewer tab as shown below.



NOTE-1: When a Business Role defined with Required Roles is requested to an Identity whose Entitlements do not match with the required Roles will be marked in red color in the identity cube as shown in the below.

NOTE-2: When a Business Role is requested to the identities in Active Directory, automatic provisioning of missing Entitlements in the Required Role is enabled in SailPointIQ.



Roles in IdentityIQ

Role Membership Certifications: 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 Role Management in IdentityIQ 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.

Scheduling a Role Membership Certification: 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.

STEP-1: GO TO ~~Monitor~~ ~~Certifications~~ ~~New~~ ~~Certification~~ ~~Role~~ ~~Membership~~

IdentityIQ

Logged in as The Administrator | Edit My Preferences | Help | Logout | SailPoint

Dashboard Define **Monitor** Analyze Manage System Setup

Certifications

Certifications Certification Schedules Certification Events

Search by Certification Name

Name	Owner	Status	Percent Complete	Create Date
Role Membership Certification [10/15/15 6:54:59 PM IST]	The Administrator	Active	0% (0 of 1)	15/10/15 18:55:00
Role Membership Certification [10/15/15 11:26:53 AM IST]	The Administrator	Active	0% (0 of 1)	15/10/15 11:26:55
Role Composition Certification [10/14/15 4:57:53 PM IST]	The Administrator	Completed	100% (1 of 1)	14/10/15 16:57:53
Application Owner Certification [10/14/15 4:52:57 PM IST]	The Administrator	Completed	100% (1 of 1)	14/10/15 16:52:57
Advanced Certification [10/1/15 4:25:06 PM IST]	The Administrator	Completed	100% (2 of 2)	01/10/15 16:25:06
Application Owner Certification [10/1/15 3:03:19 PM IST]	The Administrator	Completed	100% (1 of 1)	01/10/15 15:03:19
Application Owner Certification [10/1/15 2:43:13 PM IST]	The Administrator	Completed	100% (1 of 1)	01/10/15 14:43:14

Page 1 of 1

Displaying 1 - 7 of 7

© Copyright 2015 SailPoint Technologies - All rights reserved.

New Certification ▼

- Manager
- Application Owner
- Entitlement Owner
- Advanced
- Role Membership**
- Role Composition
- Account Group Permissions
- Account Group Membership

Roles in IdentityIQ

STEP-2: Select the Owner and the Roles to be certified, check Run now on the Basic page, In this case it is STRATEGY,

The screenshot shows the 'Schedule Certification' page in IdentityIQ, specifically the 'Basic' tab. The 'Certification Properties' section shows 'Certification Name' as 'Role Membership Certification [\${fullDate}]' and 'Certification Owner' as 'The Administrator'. Under 'What to Certify', 'Select Roles' is set to 'Manually Select Roles' with a dropdown menu showing 'STRATEGY'. Below this, 'Certify Roles by Type' is set to 'Organizational Business IT Entitlement'. Under 'When to Certify', 'Execution Frequency' is 'Once' and 'Run Now' is checked. The 'Start' date is '26 October 2015 02:11 PM'. At the bottom, there are buttons for 'Previous', 'Next', 'Schedule Certification', and 'Cancel'.

STEP-3: GO TO Behavior page; check **Enable Provisioning of Missing Role Requirements** under the decision tab. This will notify the certifier if any provisioning is required during the approval process.

The screenshot shows the 'Schedule Certification' page in IdentityIQ, specifically the 'Behavior' tab. The 'Decisions' section is highlighted, and 'Enable Provisioning Of Missing Role Requirements' is checked. Other options include 'Require Subordinate Completion', 'Automatically Sign Off When Nothing To Certify', 'Suppress Notification When Nothing To Certify', 'Require Reassignment Completion', 'Return Reassignments to Original Access Review', 'Automatically Sign Off When All Items Are Reassigned', 'Require Delegation Review', 'Require Comments For Approval', 'Require Comments When Allowing Exceptions', 'Require Bulk Certification Confirmation', 'Disable Delegation Forwarding', 'Limit Reassignments', 'Reassignment Limit', 'Enable Line Item Delegation', 'Enable Identity Delegation', 'Enable Account Approval', 'Enable Account Revocation', 'Enable Account Reassignment', 'Enable Overriding Violation Remediation', 'Enable Allow Exceptions', 'Enable Allow Exception Popup', and 'Default Duration For Exceptions'. At the bottom, there are buttons for 'Previous', 'Next', 'Schedule Certification', and 'Cancel'.

Roles in IdentityIQ

STEP-4: GO TO Advance page, select the Certifier and click on **Schedule Certification**

IdentityIQ Logged in as The Administrator | Edit My Preferences | Help | Logout

Dashboard Define Monitor Analyze Manage System Setup

Schedule Certification

Summary

Steps

1. Basic
2. Lifecycle
3. Notifications
4. Behavior
5. **Advanced**

Specify advanced options that can change the contents and behavior of the certification.

Advanced

Access Review Properties

Custom Name [?] -- Select a parameter --

Custom Short Name [?] -- Select a parameter --

Certification Assignment

Certifier(s) [?]

- ☐ Assign to Manager
- ☐ Assign to Role Owner
- ☒ Select Certifier Manually

Select Certifier Manually

[?] The Administrator

Certification Contents

Exclusion Rule [?] -- Select Rule --

Save Exclusions [?] ☐

Exclude Inactive Identities [?] ☐

Certification Rules

Pre-delegation Rule [?] -- Select Rule --

Sign Off Approver Rule [?] -- Select Rule --

« Previous Next » **Schedule Certification** Cancel

© Copyright 2015 SailPoint Technologies - All rights reserved.

STEP-5: A Work Item is created for certification; the certifier defined in the certification will be able to certify the Work Item is shown below.

IdentityIQ Logged in as The Administrator | Edit My Preferences | Help | Logout

Dashboard Define Monitor Analyze Manage System Setup

Access Review Details

Role Membership Access Review for The Administrator

Due on: 26/11/15 (31 Days remaining) | Current Phase: Active (31 Days remaining) | Percent Complete: 0/2 (0%)

Owner: The Administrator

Before you can complete the access review you must certify the access granted to each user. Select a user from the table below to certify their access or to delegate the access review to another certifier.

Filter

Legend: ● Approve ● Revoke ● Allow Exception ★ Action Required

Decision	Identity	First Name	Last Name	Description	Application	Account Name	Status	Risk Score
<input checked="" type="checkbox"/>	12	andy	jones	STRATEGY	FINANCE	12	Open	252
<input checked="" type="checkbox"/>	9	abid	hussain	STRATEGY	FINANCE	9	Open	252

Page 1 of 1 | Show 25 items | Displaying 1 - 2 of 2

-- Select Bulk Action --

Back [Show identity view](#) [Export to CSV](#)

© Copyright 2015 SailPoint Technologies - All rights reserved.

IdentityIQ

[Dashboard](#)
[Define](#)
[Monitor](#)
[Analyze](#)
[Manage](#)
[System Setup](#)

[Previous Identity](#)
[Next Identity](#)

Decisions

Recent Changes

Employee Data

Risk Data

Approve All

Revoke All

Delegate All

Clear Decisions

Legend:

Approve

Revoke

Allow Exception

Action Required

Roles

Decision

Role

STRATEGY

Missing Required Roles

Allowed Roles

Role Hierarchy

Required Roles

BUSINESS ANALYST

BUSINESS DEVELOPMENT

Permitted Roles

No Matching Roles

Provision required roles for 'STRATEGY'

Allowed Roles

Role Hierarchy

Required Roles

BUSINESS ANALYST

BUSINESS DEVELOPMENT

Role Details

Name:

STRATEGY

Type:

Business

Owner:

The Administrator

Description:

Strategy Business Role - Consulting Organization Unit

Acquired:

Assigned

Provision Required Roles

Approve Without Provisioning

Cancel

Page 1 of 1

Showing 15 items

Displaying 1 - 1 of 1

Show worksheet view

Back

© Copyright 2015 SailPoint Technologies - All rights reserved.

Roles in IdentityIQ

NOTE-1: Business Roles will be assigned to the Identities automatically by writing the **Assignment Rule** or by Access requesting in the Access Request option in the IdentityIQ Dashboard.

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 Department is one of the identity attributes, a business role can be created based on each unique Department.

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.

Creating a Business Role using Mining:

STEP-1: GO TO **Define** → **Role** → **New Role** → **Business Role Mining**, the following page is displayed. Enter the required information and click on **Save and Execute**.

Dashboard

Define

Monitor

Analyze

Manage

System Setup

Role Management

New Role

Role Viewer

Role Search

Entitlement Analysis

Role Mining

Role Mining Results

View Mining Templates

moved into either the specified existing container role or a newly generated container role.

Entitlement mining is optionally performed on the generated business roles. These entitlements are either directly attached to those business roles or moved into newly created IT roles that are added to the business roles' Permits or Requires lists, as specified.

*Indicates a required field.

General Settings

Name *

Business Role Mining

Compute Population Statistics

?

☐

Perform Analysis Only (no roles are generated)

?

☐

Hierarchical Settings

Generate a New Root Container Role

?

☒

Type of Root Container Role to Generate

?

Organizational

Generate a Role Hierarchy from the Identity Mining Attributes

?

-- Select Attribute --

Department

Ordered Identity Mining Attributes *

?

Role Settings

Type of Business Roles to Generate

?

Business

Owner *

?

-- Select an Owner --

Minimum Number of Users per Role

?

Naming Algorithm

?

☒ Filter-Based ☐ Generic UID

Prefix to Apply to Generated Role Names

?

IT Settings

Mine for Entitlements on Generated Business Roles

?

☐

Save

Save and Execute

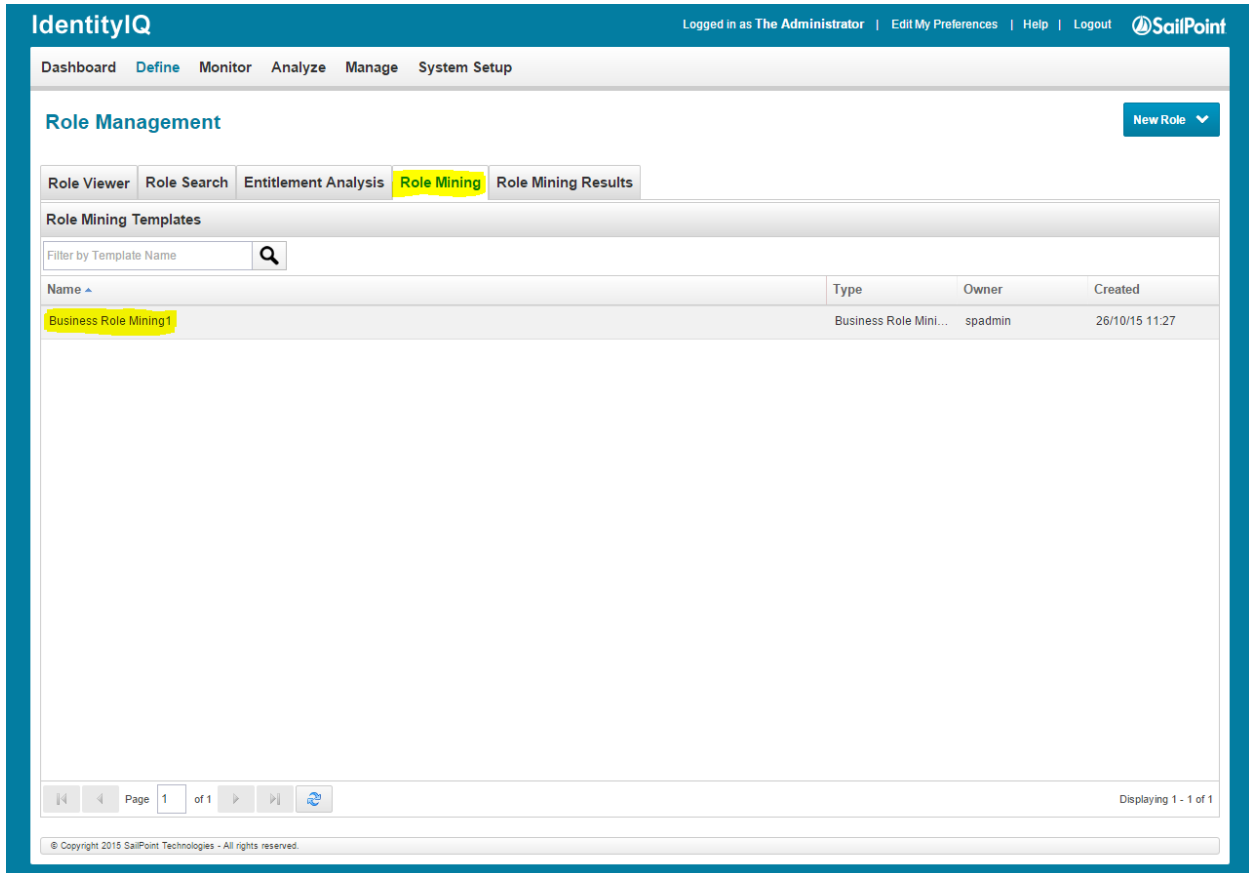
Cancel

Roles in IdentityIQ

Required fields on Role Mining Page:

1. **Name:** Name of the Role Mining.
2. **Compute Population Statistics:** Enable/Disable Population Computing Statistics.
3. **Perform Analysis Only:** Enable/Disable Perform Analysis.
4. **Type of Root Container Role to Generate:** Select the type of Role.
5. **Ordered Identity Mining Attributes:** Select the attributes from the drop down menu.
6. **Type of Business Roles to Generate:** Select the type of the Role.
7. **Owner:** Select the Owner.
8. **Minimum no of users per Role:** Specify the minimum number of users per Role.

STEP-2: After Executing the Role Mining the following page displayed with the list of Role Mines created as shown below.

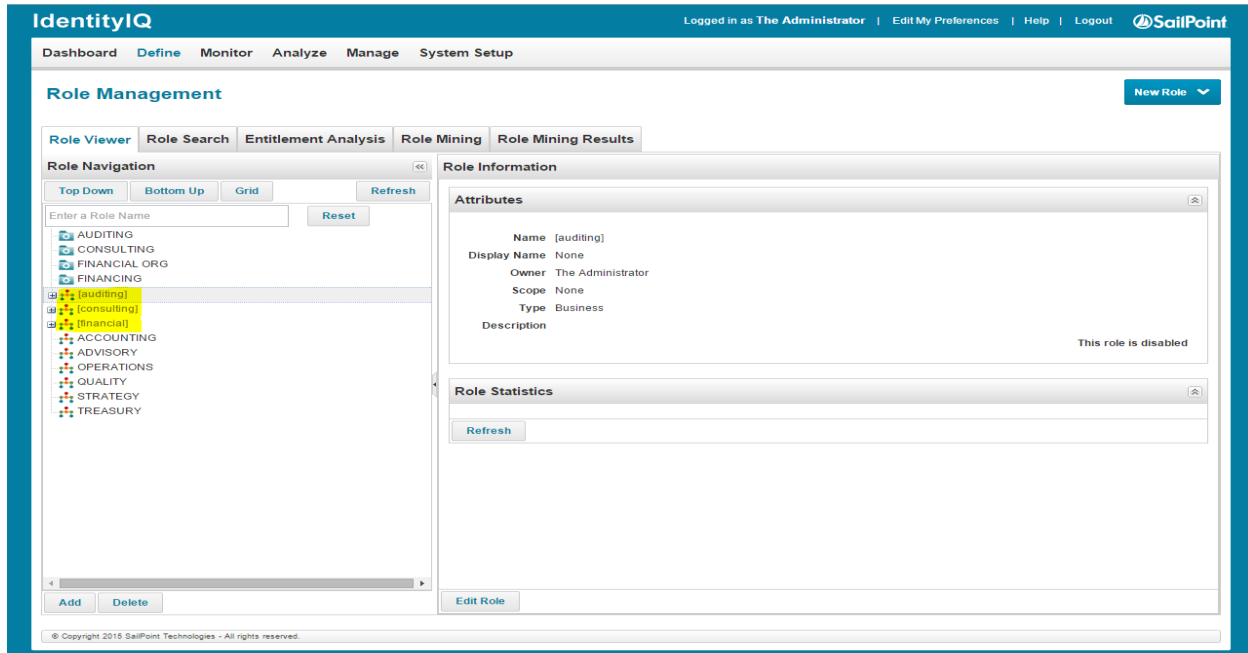


The screenshot displays the IdentityIQ web interface. At the top, the header shows 'IdentityIQ' and 'Logged in as The Administrator'. Below the header, a navigation bar includes 'Dashboard', 'Define', 'Monitor', 'Analyze', 'Manage', and 'System Setup'. The main section is titled 'Role Management' and features a 'New Role' button. A tabbed interface shows 'Role Viewer', 'Role Search', 'Entitlement Analysis', 'Role Mining' (selected), and 'Role Mining Results'. Under the 'Role Mining' tab, there is a 'Role Mining Templates' section with a search filter. A table lists the templates, with one entry highlighted: 'Business Role Mining1'. The table has columns for Name, Type, Owner, and Created.

Name	Type	Owner	Created
Business Role Mining1	Business Role Mini...	spadmin	26/10/15 11:27

The Business Role hierarchy can be viewed under Role Viewer Tab as shown in the below.

Roles in IdentityIQ



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 IdentityIQ user interface.

Impact Analysis on a Role (Business or IT Role): The impact of any changes to the Role memberships can be analyzed by submitting the role with impact analysis.

Example: Submitting a Business role with Impact Analysis.

STEP-1: GO TO **Define → Role**; select a role, click on **Edit Role** as shown in the below.

Role Editor

*Indicates a required field.

Name *

Display Name

Type *

Owner *

Description

49 of 1024 characters (including markup)

Enable Activity Monitoring ☐

Provision both profiles and policies ☐

Disabled ☐

Assignment Rule

Required Roles

Permitted Roles

Inherited Roles

Provisioning Policy

Submit Cancel Submit with Impact Analysis Check Policy Conflicts

Roles in IdentityIQ

STEP-2: Make any changes to the selected Role in this editor, like Add or Remove any Roles or change Description or inherit any Roles and click on **Submit with Impact Analysis**, a Work Item is created for Approval as shown below.

IdentityIQ

Dashboard Define Monitor Analyze Manage System Setup

Role Management

An impact analysis task has been launched for role ACCOUNTING

Role Viewer Role Search Entitlement Analysis Role Mining Role Mining Results

Role Navigation

Top Down Bottom Up Grid Refresh

Enter a Role Name Reset

- AUDITING
- CONSULTING
- FINANCIAL ORG
- FINANCING
- ACCOUNTING**
- ADVISORY
 - BFR [auditing]
 - BFR [consulting]
 - BFR [financial]
- OPERATIONS
- QUALITY
- STRATEGY
- TREASURY
- ACCOUNTS PAYABLE
- ACCOUNTS RECEIVABLE
- ADVISORS
- BUSINESS ANALYST
- BUSINESS DEVELOPMENT
- CASHIER
- FOREX
- INFORMATION MANAGEMENT
- IT ADV ROLE
- JUNIOR AUDIT

Add Delete

Role Information

Attributes

An approval or impact analysis work item is pending on this role.

Name ACCOUNTING

Display Name ACCOUNTING

Owner The Administrator

Scope None

Type Business

Description Accounting Business Role - Financing Organization

This role is enabled

Role Statistics

Refresh

Edit Role

© Copyright 2015 SailPoint Technologies - All rights reserved.

STEP-3: The Work Item for approval goes to the owner of the Role, in this case Administrator, he can view the changes made to it and the impact it has on the organization, he can approve, reject or forward to appropriate authority or identity.

IdentityIQ

Dashboard Define Monitor Analyze Manage System Setup

Role Approval

Summary

Work Item ID 27

Requester The Administrator

Owner The Administrator

Description Review impact analysis of Role: ACCOUNTING

Created 25-Oct-2015 14:37:29

Priority Normal

History None

Send Comment to Requester

None

Add Comment

Details

Name ACCOUNTING

Owner The Administrator

Description Accounting Business Role - Financing Organization

Click to view analysis task result.

Click to review pending change.

Approve Reject Forward Save Cancel

© Copyright 2015 SailPoint Technologies - All rights reserved.

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

Roles in IdentityIQ

role against the defined Policies in the system and determining if it will cause violations of any of those Policies.

Checking Policy Conflicts in a Role(Business or IT Role):

STEP-1: GO TO Define → Role; select a role, click on **EditRole** as shown in the below.

IdentityIQ

Dashboard Define Monitor Analyze Manage System Setup

Logged in as The Administrator | Edit My Preferences | Help | Logout | SailPoint

Role Editor

*Indicates a required field

Name * ACCOUNTING

Display Name ACCOUNTING

Type * Business

Owner * The Administrator

Description

Accounting Business Role - Financing Organization

49 of 1024 characters (including markup)

Enable Activity Monitoring ☐

Provision both profiles and policies ☐

Disabled ☐

Assignment Rule

None Match List Filter Script Rule Population

Required Roles

Modify Required Roles

No Required Roles

Permitted Roles

Modify Permitted Roles

No Permitted Roles

Inherited Roles

Modify Inheritance

This role does not inherit any other roles.

Provisioning Policy

Below is a list of provisioning policies associated with this role. You can add a new policy by clicking on the 'Add Provisioning Policy' button below or edit an existing one by clicking on it in the list.

There are currently no provisioning policies defined.

Add Provisioning Policy Delete Provisioning Policy

Submit Cancel Submit with Impact Analysis Check Policy Conflicts

© Copyright 2015 SailPoint Technologies - All rights reserved.

STEP-2: Click on **Check Policy Conflicts**, we can find out if this Role has any conflicts with the policies defined in the IdentityIQ.

Permitted Roles

Modify Permitted Roles

No Permitted Roles

Inherited Roles

Modify Inheritance

This role does not inherit any other roles.

Provisioning Policy

Below is a list of provisioning policies associated with this role. You can add a new policy by clicking on the 'Add Provisioning Policy' button below or edit an existing one by clicking on it in the list.

There are currently no provisioning policies defined.

Add Provisioning Policy

Policy Conflicts

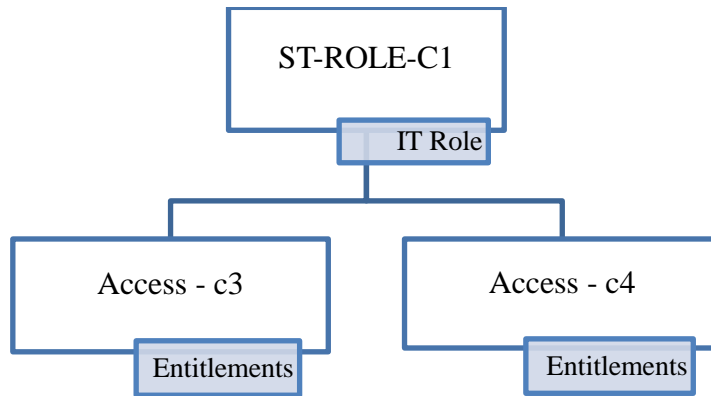
No policy conflicts found.

Submit Cancel Submit with Impact Analysis Check Policy Conflicts

Roles in IdentityIQ

3. **IT Role:** IT Roles allow multiple entitlements from one or more applications to be grouped together into a single role. IT roles should encapsulate groups of related entitlements that are shared by one or more business roles.

Example:



In the above figure BUSINESS ANALYST is an IT Role created for the Identities who are all entitled with the Access c3 & c4.

Creation of an IT Role:

STEP-1:GO TO Define - > Roles, the following screen is displayed as shown

The screenshot shows the IdentityIQ Role Management interface. The 'Role Information' tab is selected, displaying the following details for the 'ACCOUNTING' role:

- Attributes:**
 - Name: ACCOUNTING
 - Display Name: ACCOUNTING
 - Owner: The Administrator
 - Scope: None
 - Type: Business
 - Description: Accounting Business Role - Financing Organization
- Role Statistics:** (Empty table with a 'Refresh' button)

The role is marked as 'This role is enabled'. The interface also includes a 'Role Navigation' pane on the left with a tree view of roles, and a 'New Role' button in the top right corner.

Roles in IdentityIQ

STEP-2: Click on **New Role** and select **Role**, the following screen is displayed. Enter the required fields and click on **Submit**.

IdentityIQ Logged in as **The Administrator** | Edit My Preferences | Help | Logout | **SailPoint**

Dashboard **Define** Monitor Analyze Manage System Setup

Role Editor

*Indicates a required field.

Name *

Display Name

Type *

Owner *

Description

B **I** **U** **Link** **Unlink** **Language** **English (United States)**

ST-ROLE-C1 - IT ROLE- STRATEGY BUS Group

40 of 1024 characters (including markup)

Enable Activity Monitoring ☐

Provision both profiles and policies ☐

Disabled ☐

Inherited Roles

[Modify Inheritance](#)

This role does not inherit any other roles.

Entitlements

[Add](#) [Advanced View](#)

Application	Property	Value
No data to display		

Provisioning Policy

Below is a list of provisioning policies associated with this role. You can add a new policy by clicking on the 'Add Provisioning Policy' button below or edit an existing one by clicking on it in the list.

There are currently no provisioning policies defined.

[Add Provisioning Policy](#) [Delete Provisioning Policy](#)

Provisioning Target Account Selector Rules

General Rule

[Submit](#) [Cancel](#) [Submit with Impact Analysis](#) [Check Policy Conflicts](#)

© Copyright 2015 SailPoint Technologies - All rights reserved.

Required Fields on Role Editor Page:

1. **Name:** Name of the IT Role.
2. **Display Name:** Display Name for the IT Role.
3. **Type:** Select type as **IT** from the drop down menu.
4. **Owner:** select the Owner for the IT Role.
5. **Description:** Description for the IT Role.
6. **Enable Activity Monitoring:** To enable/disable the Activity Monitoring.
7. **Disabled:** Enable/Disable the Role.
8. **Inherited Roles:** To inherit any other roles, click on **modify Inheritance**.
9. **Entitlements:** Select the Entitlements you want to group them as a role.

Roles in IdentityIQ

STEP-3: To add the entitlements click on **Add** option under the Entitlements a new window is popped up as shown in the below.

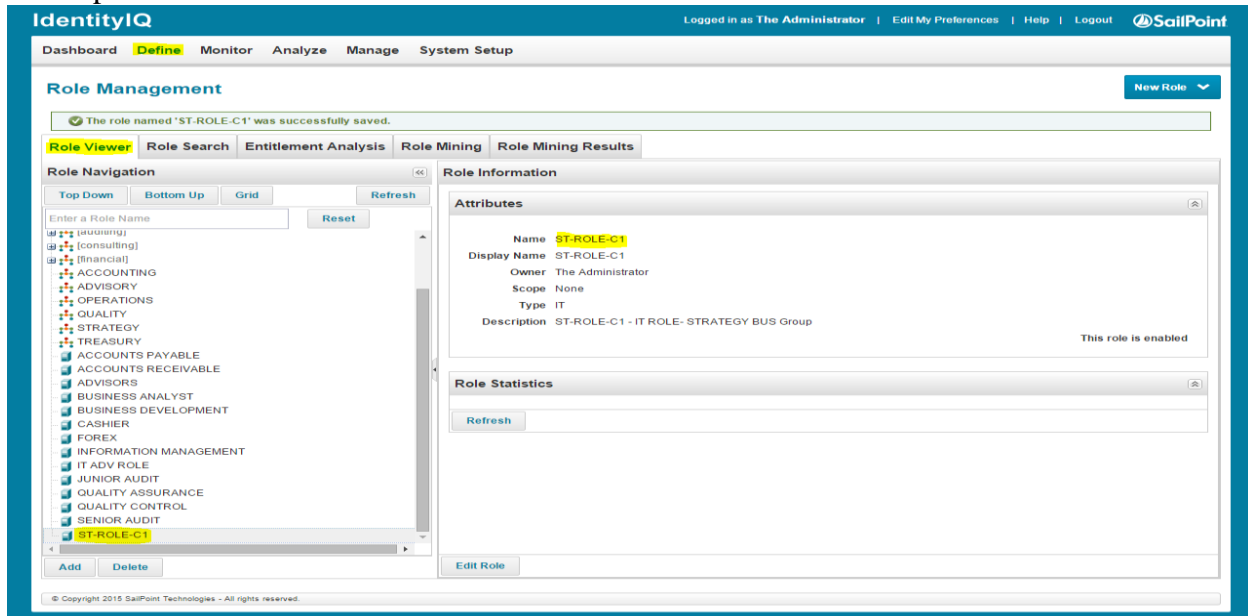
The screenshot shows the IdentityIQ Role Editor interface. The main form has fields for Name (ST-ROLE-C1), Display Name (ST-ROLE-C1), Type, Owner, and Description. Below these are checkboxes for 'Enable Activity Monitoring' and 'Provision both profiles and policies'. The 'Entitlements' section is highlighted in yellow, and the 'Add' button is also highlighted. A modal dialog titled 'Edit Entitlements' is open, showing a table with columns 'Application', 'Property', and 'Value'. The 'Application' column has a dropdown menu. The dialog has 'Save' and 'Cancel' buttons at the bottom.

STEP-4: Select the **Application** from the drop down menu and the **Entitlements** you want to group as a Role and click on **Save** and click on **Submit**.

The screenshot shows the IdentityIQ Role Editor interface. The main form has fields for Name (ST-ROLE-C1), Display Name (ST-ROLE-C1), Type, Owner, and Description. Below these are checkboxes for 'Enable Activity Monitoring' and 'Provision both profiles and policies'. The 'Entitlements' section is highlighted in yellow, and the 'Add' button is also highlighted. A modal dialog titled 'Edit Entitlements' is open, showing a table with columns 'Application', 'Property', and 'Value'. The 'Application' column has a dropdown menu with 'FINANCE' selected. The dialog has 'Save' and 'Cancel' buttons at the bottom.

Roles in IdentityIQ

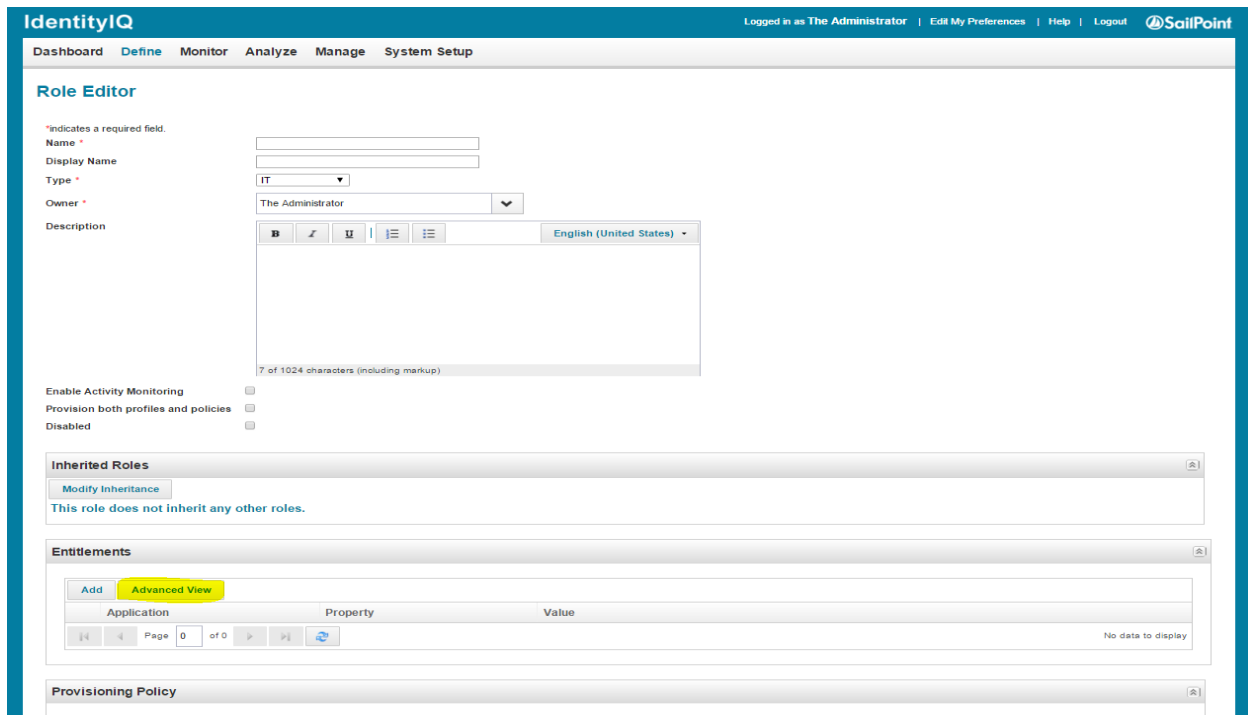
The roles you have created will be listed down under the **Role Viewer** menu as shown in the below picture.



NOTE: IT Roles will be automatically detected to the matched Identities on Refreshing the Identity Cube by checking **Refresh assigned, detected roles and promote additional entitlements**.

Creation of an IT Role using Profiles in Advance View option: Here we will discover creating an IT Role using Profiles in the Advance View option.

STEP-1:GO TO Define -Roles New RoleRole. →



Roles in IdentityIQ

STEP-2: Select Advance View in the Entitlements window the following screen is displayed
Select **Create** → **New Profile** as shown below.

The screenshot shows the IdentityIQ Role Editor interface. The top navigation bar includes 'Dashboard', 'Define', 'Monitor', 'Analyze', 'Manage', and 'System Setup'. The 'Define' tab is active. The 'Role Editor' section contains fields for 'Name', 'Display Name', 'Type', 'Owner', and 'Description'. The 'Name' and 'Display Name' fields are both set to 'IT ADV ROLE'. The 'Type' is set to 'IT'. The 'Owner' is 'The Administrator'. The 'Description' field is empty. Below these fields are checkboxes for 'Enable Activity Monitoring', 'Provision both profiles and policies', and 'Disabled'. The 'Inherited Roles' section shows 'This role does not inherit any other roles.' The 'Entitlements' section has a 'Create' button highlighted, with a dropdown menu showing 'New Profile' and 'New Profile from Entitlement Analysis'. The 'Provisioning Policy' section shows 'There are currently no provisioning policies defined.'

STEP-3: Edit Entitlement page is displayed, select the Application, add the filters and save it.

The screenshot shows the IdentityIQ Role Editor interface with the 'Edit Entitlements' dialog box open. The dialog box has a 'Description' field, an 'Application' dropdown set to 'FINANCE', and an 'Attribute Rules' section. The 'Add A Filter' section is active, showing a table with columns 'Field', 'Search Type', 'Value', and 'Ignore Case'. The table contains two rows: one with 'ACCESS' in the Field column, 'contains all' in the Search Type column, and 'x1' in the Value column; and another with 'ACCESS' in the Field column, 'contains all' in the Search Type column, and 'x2' in the Value column. The 'Ignore Case' column is empty. Below the table is an 'Add Filter' button. At the bottom of the dialog box, there is a 'Save' button and a 'Cancel' button. The background shows the same Role Editor page as in the previous screenshot, but the 'Create' button is no longer highlighted.

Roles in IdentityIQ

STEP-4: It redirects back to the Role Editor page, go ahead and submit it, you can view all the created roles under Role viewer tab.

IdentityIQ Logged in as The Administrator | Edit My Preferences | Help | Logout | SailPoint

Dashboard Define Monitor Analyze Manage System Setup

Role Editor

*Indicates a required field.

Name * IT ADV ROLE

Display Name IT ADV ROLE

Type * IT

Owner * The Administrator

Description

7 of 1024 characters (including markup)

Enable Activity Monitoring ☐

Provision both profiles and policies ☐

Disabled ☐

Inherited Roles

Modify Inheritance

This role does not inherit any other roles.

Entitlements

Create Simple View

Entitlements for Account on FINANCE [Edit] [Delete]

Rule

ACCESS.containsAll("a1", "a2")

Provisioning Policy

Below is a list of provisioning policies associated with this role. You can add a new policy by clicking on the 'Add Provisioning Policy' button below or edit an existing one by clicking on it in the list.

There are currently no provisioning policies defined.

Add Provisioning Policy Delete Provisioning Policy

Provisioning Target Account Selector Rules

General Rule -- Select Rule --

FINANCE -- Select Rule --

Submit Cancel Submit with Impact Analysis Check Policy Conflicts

© Copyright 2015 SailPoint Technologies - All rights reserved.

Creating IT Roles using Profiles created From Entitlement Analysis in

Advance View option: Profiles can also be created from Entitlement Analysis in Advance View tab in Role Editor Page.

Roles in IdentityIQ

STEP-1: GO TO **Define** → **Roles** → **New Role**

IdentityIQ

Logged in as The Administrator | Edit My Preferences | Help | Logout

SailPoint

Dashboard

Define

Monitor

Analyze

Manage

System Setup

Role Editor

*Indicates a required field.

Name *

IT ROLE ENT

Rectangular Snip

Display Name

IT ROLE ENT

Type *

IT

Owner *

The Administrator

Description

B

I

U

L

I

I

I

English (United States)

7 of 1024 characters (including markup)

Enable Activity Monitoring

Provision both profiles and policies

Disabled

Inherited Roles

Modify Inheritance

This role does not inherit any other roles.

Entitlements

Create

Simple View

New Profile

New Profile from Entitlement Analysis

Provisioning Policy

Below is a list of provisioning policies associated with this role. You can add a new policy by clicking on the 'Add Provisioning Policy' button below or edit an existing one by clicking on it in the list.

There are currently no provisioning policies defined.

Roles in IdentityIQ

STEP-2: Select Advance View in the Entitlements window the following screen is displayed
Select **Create** → **New Profile from Entitlement Analysis** as shown below.

The screenshot shows the IdentityIQ Role Editor interface. At the top, the 'Role Editor' tab is active. Below it, the 'Create Profiles from Entitlement Analysis' window is open. This window contains several sections: a top section for role details (Name, Display Name, Type), a 'Filter Operation' section with a dropdown set to 'And', a 'Search By' section with radio buttons for 'Attributes' and 'Population', and a main section for selecting attributes. The 'Identity Attributes' section is divided into 'Standard Attributes' (Last Name, First Name, Username, Display Name, Email, Manager) and 'Searchable Attributes' (ROLLNO, Department, Access, First Name). Each attribute has a corresponding input field or dropdown. At the bottom of the window, there is a 'Provisioning Policy' section with a message stating 'There are currently no provisioning policies defined.' and buttons for 'Add Provisioning Policy' and 'Edit Provisioning Policy'.

STEP-3: Enter the name, description, type, and select the **Application**, and their **Attributes**, click on **Search** as shown below.

This screenshot is identical to the previous one, but with the 'Application' dropdown menu in the 'Create Profiles from Entitlement Analysis' window open. The 'FINANCE' option is highlighted in yellow. The 'Search' button at the bottom right of the window is also highlighted in green.

Roles in IdentityIQ

STEP-4: The search results are displayed as shown below, select the required Entitlements and click on **Create profile** and click on **Save**.

IdentityIQ

Logged in as The Administrator | Edit My Preferences | Help | Logout

SailPoint

Dashboard

Define

Monitor

Analyze

Manage

System Setup

Role Editor

*Indicates a required field.

Name *

IT ROLE ENT

Display Name

IT ROLE ENT

Type *

IT

Create Profiles from Entitlement Analysis

Export to CSV

Search Parameters

Attribute	Filter Type	Value(s)
Applications	Equal	FINANCE

Only show percentages above

0

FINANCE - Entitlement Attributes

<input type="checkbox"/>	Name	Value	Percent of Population
<input checked="" type="checkbox"/>	DEPARTMENT	auditing	4/12 (33%)
<input checked="" type="checkbox"/>	DEPARTMENT	consulting	4/12 (33%)
<input checked="" type="checkbox"/>	DEPARTMENT	financial	4/12 (33%)
<input type="checkbox"/>	LOCATION	uk	4/12 (33%)
<input type="checkbox"/>	LOCATION	usa	4/12 (33%)
<input type="checkbox"/>	LOCATION	swedan	2/12 (17%)

Group and Analyze

Refine Search

Create Profiles

Cancel

Provisioning Policy

Below is a list of provisioning policies associated with this role. You can add a new policy by clicking on the 'Add Provisioning Policy' button below or edit an existing one by clicking on it in the list.

There are currently no provisioning policies defined.

IdentityIQ

Logged in as The Administrator | Edit My Preferences | Help | Logout

SailPoint

Dashboard

Define

Monitor

Analyze

Manage

System Setup

Role Editor

*Indicates a required field.

Name *

IT ROLE ENT

Display Name

IT ROLE ENT

Type *

IT

Create Profiles from Entitlement Analysis

Description

Profile(s) will be created for the following entitlement(s):

FINANCE Entitlements

Name	Value
DEPARTMENT	auditing
DEPARTMENT	consulting
DEPARTMENT	financial

Save

Cancel

Provisioning Policy

Below is a list of provisioning policies associated with this role. You can add a new policy by clicking on the 'Add Provisioning Policy' button below or edit an existing one by clicking on it in the list.

There are currently no provisioning policies defined.

Roles in IdentityIQ

STEP-5: It redirects to the Role Editor page, Click on Submit, IT role is created using Profiles created from Entitlement Analysis. As shown below.

IdentityIQ

Logged in as The Administrator | Edit My Preferences | Help | Logout

Dashboard

Define

Monitor

Analyze

Manage

System Setup

Role Editor

*Indicates a required field.

Name *

IT ROLE ENT

Display Name

IT ROLE ENT

Type *

IT

Owner *

The Administrator

Description

B

I

U

☰

☷

English (United States)

7 of 1024 characters (including markup)

Enable Activity Monitoring

☐

Provision both profiles and policies

☐

Disabled

☐

Inherited Roles

Modify Inheritance

This role does not inherit any other roles.

Entitlements

DEPARTMENT.containsAll({"auditing", "consulting", "financial"})

Provisioning Policy

Below is a list of provisioning policies associated with this role. You can add a new policy by clicking on the 'Add Provisioning Policy' button below or edit an existing one by clicking on it in the list.

There are currently no provisioning policies defined.

Add Provisioning Policy

Delete Provisioning Policy

Provisioning Target Account Selector Rules

General Rule

-- Select Rule --

...

Submit

Cancel

Submit with Impact Analysis

Check Policy Conflicts

© Copyright 2015 SailPoint Technologies - All rights reserved.

Roles in IdentityIQ

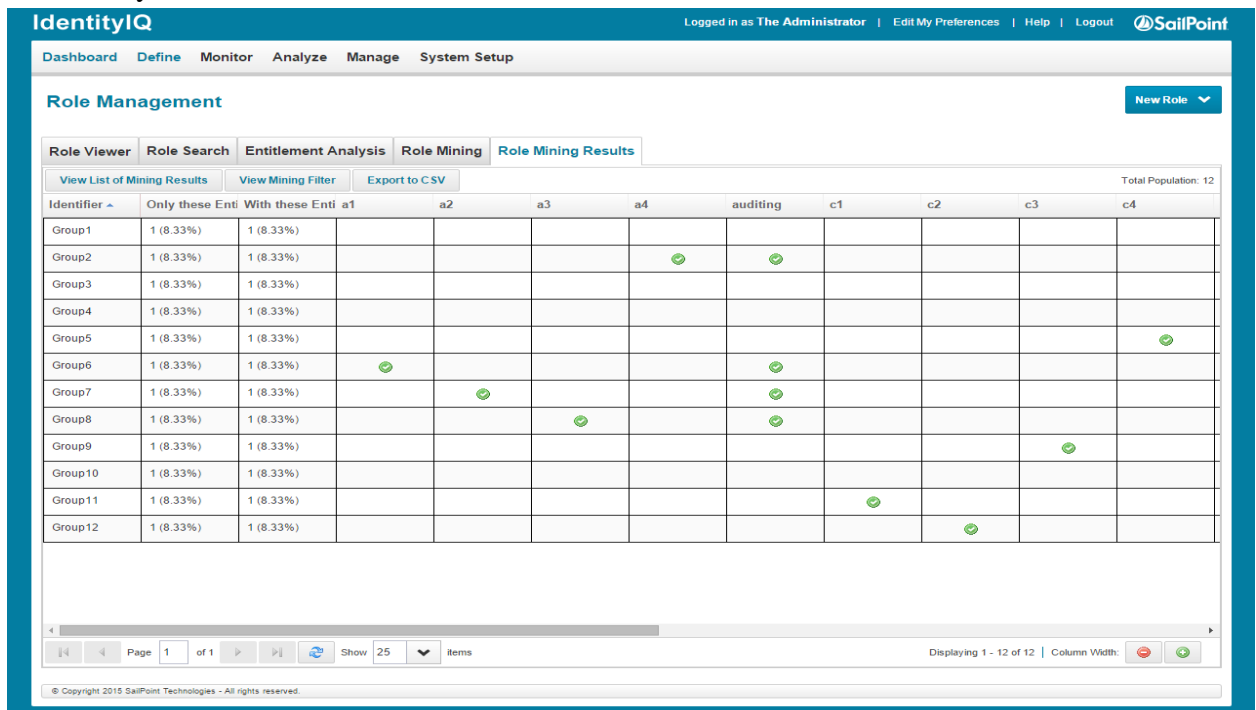
IT Roles can be created automatically by setting up the filters in IT Role Mining.

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 or by running an Entitlement Analysis.

IT Role Mining: 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.

- Administrator selects one or more application whose entitlements will be evaluated as well as set of identity attributes that filter the identities that should be examined.
- IT Role Mining is designed to highlight identities entitlements commonalities. Returns every set of entitlements on the selected applications that are all held by one or more identities.
- It does not return subsets where there are no identities.
- IT role mining definitions and results can be saved and to be re-run or examined later.
- Roles created from IT role mining are created in disabled state and must be enabled before they will be detected for a user.



Identifier	Only these Enti	With these Enti	a1	a2	a3	a4	auditing	c1	c2	c3	c4
Group1	1 (8.33%)	1 (8.33%)									
Group2	1 (8.33%)	1 (8.33%)				✓	✓				
Group3	1 (8.33%)	1 (8.33%)									
Group4	1 (8.33%)	1 (8.33%)									
Group5	1 (8.33%)	1 (8.33%)									✓
Group6	1 (8.33%)	1 (8.33%)	✓				✓				
Group7	1 (8.33%)	1 (8.33%)		✓			✓				
Group8	1 (8.33%)	1 (8.33%)			✓		✓				
Group9	1 (8.33%)	1 (8.33%)								✓	
Group10	1 (8.33%)	1 (8.33%)									
Group11	1 (8.33%)	1 (8.33%)						✓			
Group12	1 (8.33%)	1 (8.33%)							✓		

Roles in IdentityIQ

An Example for IT Role Mining: We will create an IT role using IT Role Mining as shown in the below steps.

STEP-1: GO TO Define → Role → New Role → IT Role Mining, the following page is displayed. Enter the required information and click on **Save and Execute**.

The screenshot shows the IdentityIQ Role Management interface. The top navigation bar includes 'Dashboard', 'Define', 'Monitor', 'Analyze', 'Manage', and 'System Setup'. The 'Define' tab is active, and the 'Role Management' section is selected. The 'Role Mining' sub-tab is active, showing the 'IT Role Mining' configuration page. The page includes fields for 'Name' (IT ROLE MINING), 'Owner' (The Administrator), 'Identities to Mine' (Search By Attributes), 'Applications to Mine' (FINANCE), and 'Entitlements to Exclude'. The 'Save and Execute' button is highlighted.

Required fields on Role Mining Page:

1. **Name:** Name of the Role Mining.
2. **Owner:** Select the Owner for the mining.
3. **Identities to Mine:** Filter the Identities for mining, this can be done by two ways
 - Search by Attributes
 - Search by Population
4. **Applications to Mine:** Select the application for mining.
5. **Entitlements to Exclude:** Select the entitlements for the selected application to be excluded from mining.
6. **Minimum identities per Role:** Specify the minimum number of identities per role.
7. **Minimum Entitlements per Role:** Specify the minimum number of Entitlements per role.
8. **Maximum Groups to Mine:** Specify Maximum number of groups to be mined.

Roles in IdentityIQ

STEP-2: After Executing the Role Mining the following page displayed with the list of Role Mines created as shown below.

The screenshot shows the IdentityIQ Role Management interface. The top navigation bar includes 'Dashboard', 'Define', 'Monitor', 'Analyze', 'Manage', and 'System Setup'. The 'Role Management' section is active, with tabs for 'Role Viewer', 'Role Search', 'Entitlement Analysis', 'Role Mining', and 'Role Mining Results'. The 'Role Mining Templates' section is displayed, featuring a search bar and a table of templates. The table has columns for Name, Type, Owner, and Created. Two templates are listed: 'Business Role Mining1' and 'IT ROLE MINING1' (highlighted in yellow). The bottom of the page shows pagination information: 'Page 1 of 1' and 'Displaying 1 - 2 of 2'.

Name	Type	Owner	Created
Business Role Mining1	Business Role Mini...	spadmin	26/10/15 11:27
IT ROLE MINING1	IT Role Mining	spadmin	26/10/15 13:22

STEP-3: The results for the Role Mining can be viewed in **Role Mining Results** tab as shown below.

The screenshot shows the IdentityIQ Role Mining Results interface. The top navigation bar is the same as in the previous screenshot. The 'Role Mining Results' tab is active, displaying a table of results. The table has columns for Identifier, Only these Enti, With these Enti, a1, a2, a3, a4, auditing, c1, c2, c3, and c4. The table contains 12 rows of data, each representing a group. The bottom of the page shows pagination information: 'Page 1 of 1' and 'Displaying 1 - 12 of 12'.

Identifier	Only these Enti	With these Enti	a1	a2	a3	a4	auditing	c1	c2	c3	c4
Group1	1 (8.33%)	1 (8.33%)									
Group2	1 (8.33%)	1 (8.33%)				✓	✓				
Group3	1 (8.33%)	1 (8.33%)									
Group4	1 (8.33%)	1 (8.33%)									
Group5	1 (8.33%)	1 (8.33%)									✓
Group6	1 (8.33%)	1 (8.33%)	✓				✓				
Group7	1 (8.33%)	1 (8.33%)		✓			✓				
Group8	1 (8.33%)	1 (8.33%)			✓		✓				
Group9	1 (8.33%)	1 (8.33%)								✓	
Group10	1 (8.33%)	1 (8.33%)									
Group11	1 (8.33%)	1 (8.33%)						✓			
Group12	1 (8.33%)	1 (8.33%)							✓		

[illegible]

Roles in IdentityIQ

Required fields for Create Role window:

1. **Name:** Name of the IT role.
2. **Owner:** Select the Owner for the IT Role.
3. **Scope:** Select the Scope from the drop down menu.
4. **Container Role:** Select the Container Role.
5. **Description:** Description for the IT Role.
6. **Entitlements to Include:** Entitlements Included will be displayed here.
7. **Inherited Roles:** Select the Roles to be inherited.
8. **Entitlements from Inherited Roles:** Entitlements for the Inherited Roles will be displayed here.

STEP-6: The system generated IT Role through Role Mining will be listed down under the **Role Viewer** tab as shown.

The screenshot displays the IdentityIQ Role Management interface. At the top, a navigation bar includes 'Dashboard', 'Define', 'Monitor', 'Analyze', 'Manage', and 'System Setup'. The 'Define' tab is active, showing 'Role Management'. A 'New Role' button is in the top right. A green message bar states: 'The role named 'ENT - Analysis Role' was successfully saved.'

The interface is divided into two main sections: 'Role Navigation' on the left and 'Role Information' on the right.

Role Navigation: Features a search bar 'Enter a Role Name' with a 'Reset' button. Below is a tree view of roles. The 'ENT - Analysis Role' is highlighted. Other roles include ACCOUNTING, ADVISORY, BFR [auditing], BFR [consulting], BFR [financial], OPERATIONS, QUALITY, STRATEGY, TREASURY, ACCOUNTS PAYABLE, ACCOUNTS RECEIVABLE, ADVISORS, BUSINESS ANALYST, BUSINESS DEVELOPMENT, CASHIER, FOREX, INFORMATION MANAGEMENT, IT ADV ROLE, JUNIOR AUDIT, QUALITY ASSURANCE, QUALITY CONTROL, and SENIOR AUDIT. At the bottom are 'Add' and 'Delete' buttons.

Role Information: Contains three panels:

- Attributes:** Lists role details: Name (ENT - Analysis Role), Display Name (None), Owner (The Administrator), Scope (None), Type (IT), and Description. A status 'This role is enabled' is shown at the bottom right.
- Role Statistics:** Includes a 'Refresh' button.
- Direct Entitlements:** A table showing entitlements for the role.

Application	Property	Value
FINANCE	ACCESS	a1
FINANCE	LOCATION	uk
FINANCE	DEPARTMENT	auditing

An 'Edit Role' button is located at the bottom of the 'Direct Entitlements' panel.

At the very bottom, a copyright notice reads: '© Copyright 2015 SailPoint Technologies - All rights reserved.'

Roles in IdentityIQ

Entitlement Analysis: 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. However, Entitlement Analysis does not show the existing connections between entitlements as well as IT Role Mining does.

An Example for Entitlement Analysis:

STEP-1: GO TO Define → Role → New Role → Entitlement Analysis, the following page is displayed. Enter the required information and click on **Search**.

The screenshot shows the IdentityIQ web interface. The top navigation bar includes 'Dashboard', 'Define', 'Monitor', 'Analyze', 'Manage', and 'System Setup'. The 'Define' tab is active, and the 'Role Management' section is selected. Within 'Role Management', the 'Entitlement Analysis' tab is highlighted. The page contains a form for configuring a new role. It includes a 'Role Viewer' tab, a 'Role Search' tab, and a 'Role Mining' tab. The 'Entitlement Analysis' tab is active. The form has a 'Please choose an application from the list below to mine for entitlements. If you would like to narrow the list of identities that is used to query for entitlements, fill in any of the search additional search fields.' instruction. There is a dropdown menu for 'Application:' with 'FINANCE' selected. To the right, there is a 'Filter Operation:' section with a description: 'Determines whether the identities returned will be based on if they have accounts on all applications selected ("AND") or any of the applications selected ("OR").' and a dropdown menu set to 'And'. Below this, there are radio buttons for 'Search By Attributes' (selected) and 'Search By Population'. The 'Identity Attributes' section is divided into 'Standard Attributes' and 'Searchable Attributes'. 'Standard Attributes' includes fields for Last Name, First Name, Username, Display Name, Email, Manager, and Is Inactive. 'Searchable Attributes' includes fields for ROLLNO, Department, Access, and First Name. At the bottom, there are 'Search' and 'Reset' buttons. The footer shows the copyright notice: '© Copyright 2015 SailPoint Technologies - All rights reserved.'

Required fields on Role Mining Page:

1. **Application:** Select the Application for analysis.
2. **Filter Operation:** Select the Owner for the mining.
3. **Identities to Mine:** Determines whether the identities returned will be based on if they have accounts on all applications selected ("AND") or any of the applications selected ("OR").

Roles in IdentityIQ

STEP-2: The search results are displayed as shown in the below.

The screenshot shows the IdentityIQ Role Management interface. The 'Entitlement Analysis' tab is selected. The search parameters are set to 'Applications' with a filter type of 'Equal' and a value of 'FINANCE'. The 'Only show percentages above' slider is set to 0. The results table, titled 'FINANCE - Entitlement Attributes', lists various attributes and their values, along with a bar chart and percentage for each. The 'Create Role' button is highlighted in yellow.

Name	Value	Percent of Population
DEPARTMENT	auditing	4/12 (33%)
DEPARTMENT	consulting	4/12 (33%)
DEPARTMENT	financial	4/12 (33%)
LOCATION	uk	4/12 (33%)
LOCATION	usa	4/12 (33%)
LOCATION	swedan	2/12 (17%)
ACCESS	a1	1/12 (8%)
ACCESS	a2	1/12 (8%)

STEP-3: Select the Entitlements you want to group together and click on **Create Role** as shown below.

The screenshot shows the IdentityIQ Role Management interface. The 'Entitlement Analysis' tab is selected. The search parameters are set to 'Applications' with a filter type of 'Equal' and a value of 'FINANCE'. The 'Only show percentages above' slider is set to 0. The results table, titled 'FINANCE - Entitlement Attributes', lists various attributes and their values, along with a bar chart and percentage for each. The 'Create Role' button is highlighted in yellow.

Name	Value	Percent of Population
DEPARTMENT	auditing	4/12 (33%)
DEPARTMENT	consulting	4/12 (33%)
DEPARTMENT	financial	4/12 (33%)
LOCATION	uk	4/12 (33%)
LOCATION	usa	4/12 (33%)
LOCATION	swedan	2/12 (17%)
ACCESS	a1	1/12 (8%)
ACCESS	a2	1/12 (8%)

IdentityIQ Logged in as The Administrator | [Edit My Preferences](#) | [Help](#) | [Logout](#) 



IdentityIQ | Logged in as The Administrator | Edit My Preferences | Help | Logout |

