



# Best Practices: When to Use Logical Applications vs Roles

---

IdentityIQ Version 6.0, 6.1

*This document provides Best Practices information that can help in the decision about whether to use a Role or a Logical Application to model access.*

© Copyright 2012 SailPoint Technologies, Inc., All Rights Reserved.

SailPoint Technologies, Inc. makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SailPoint Technologies shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

**Restricted Rights Legend.** All rights are reserved. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of SailPoint Technologies. The information contained in this document is subject to change without notice.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

**Regulatory/Export Compliance.** The export and reexport of this software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or reexport outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Government's Entities List; a party prohibited from participation in export or reexport transactions by a U.S. Government General Order; a party listed by the U.S. Government's Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

**Trademark Notices.** Copyright © 2012 SailPoint Technologies, Inc. All rights reserved. SailPoint, the SailPoint logo, SailPoint IdentityIQ, and SailPoint Identity Analyzer are trademarks of SailPoint Technologies, Inc. and may not be used without the prior express written permission of SailPoint Technologies, Inc. All other trademarks shown herein are owned by the respective companies or persons indicated.

## Table of Contents

Overview of Logical Applications and Roles.....	4
What is a Logical Application?.....	4
What is a Role?.....	4
Similarities and Differences.....	5
General Recommendations.....	5
Decision Considerations.....	5
What is Being Modeled.....	5
Performance Impacts.....	7
Logical Applications Performance Considerations.....	7
Role Performance Considerations.....	8
Ease of Configuration.....	9
Logical Applications.....	9
Roles.....	10
Provisioning Flexibility.....	11
Logical Applications.....	11
Roles.....	12
Other Resources.....	14

## Overview of Logical Applications and Roles

### What is a Logical Application?

Traditionally, enterprise applications are accessed by entering a username and password configured specifically for that application.

Access to some applications, however, is granted when certain conditions have been met by other applications. For example, employees can access a web-based time tracking system when they are members of the LDAP group "OU=employees,DC=sailpoint,DC=com" and they have an account on the Oracle HR database. This latter type of application can be modeled as a Logical Application in IdentityIQ.

There are two distinct types of use cases for Logical Applications. The first and simplest type can be thought of as a "subdivide" use case. When a subset of the attributes on some application account have a specific set of values, then a Logical Application account is created for that identity. For example, access to the Logical Application 'Sailpoint' is assigned to any identity with an Active Directory account having a groupmbr attribute value that starts with the string "Sail".

The second and more complex type of use case is usually referred to as "composite". This use case allows access to a Logical Application when an identity has some specified combination of accounts on multiple other applications. The time tracking web application described above is an example of the composite use case, with its requirements for both an LDAP and Oracle account.

### What is a Role?

Roles are similar to Logical Applications in that they can encapsulate the entitlements needed to access enterprise applications. Roles can provide another layer of abstraction, though, by mapping these entitlements to business-friendly job functions.

Roles can be used to model the structure and business operations of an enterprise. When Roles are configured to model job junctions, provisioning and deprovisioning can be significantly streamlined. For example, the onboarding of a new employee could be accomplished by the assignment of a single Business Role encapsulating all the application access and entitlements required to perform their job function. When this employee changes jobs, a new Role assignment can automatically deprovision the entitlements they no longer require and assign all the new access appropriate for their new job function.

The most commonly used default role types are:

- **Organizational:** describe the company's organizational structure
- **Business:** identify job functions or titles
- **IT:** encapsulate sets of system entitlements

An IT Role directly represents sets of system access or entitlements, which can span multiple applications. The entitlement profile for an IT Role can include Logical Applications.

Refer to the Whitepaper titled " Role Management in IdentityIQ" for a detailed discussion of the rich features and benefits available with IdentityIQ Roles.

## Similarities and Differences

Logical Applications and Roles have a number of similarities.

- Both are abstractions.
- They provide a way to manage user access to critical applications and systems.
- They can simplify the provisioning and certification processes by encapsulating entitlements and permissions in a single unit.
- They can present entitlement data in a way that is more easily understood by non-technical reviewers.

The primary differences between Logical Applications and Roles are:

- They provide different ways of modeling access. Logical Applications are account-centric, while Roles are entitlement-centric.
- Roles have an extended set of features not available to Logical Applications including:
  - Automated creation and management through role mining, entitlement analysis, impact analysis, role inheritance, and role archiving
  - Management through workflows that can create/update/delete roles, schedule role creation and decommissioning, and schedule role/entitlement assignment
- Roles scale significantly better than Logical Applications. Refer to the section titled Performance Impacts below for more details about the scalability of Logical Applications and Roles.

## General Recommendations

The decision to use a Logical Application or a Role should be based both on the business problem to be solved and the resources available to solve it. In general, Roles are easier to implement and manage than Logical Applications. However, a Logical Application may be the preferred choice for customers who want to certify and provision sets of entitlements in a way consistent with their Application Account processes. Logical Applications and Roles can be used together to model access.

## Decision Considerations

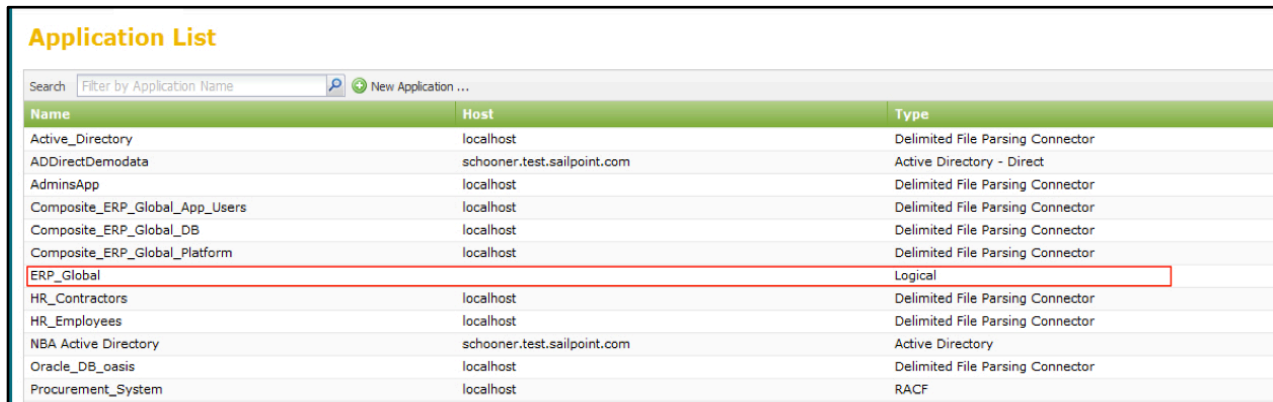
When deciding whether to use Logical Applications or Roles, these are the key factors to consider.

### What is Being Modeled

Logical Applications are designed to model application accounts. Roles, with their additional functionality and flexibility, are designed to model entitlements based on an organization's business structure and operations.

Historically, user accounts with their accompanying passwords have been used as the means to protect access to application and system resources. The past decade, however, has seen the advent of web applications and single-sign-on solutions that have new authentication and authorization mechanisms.

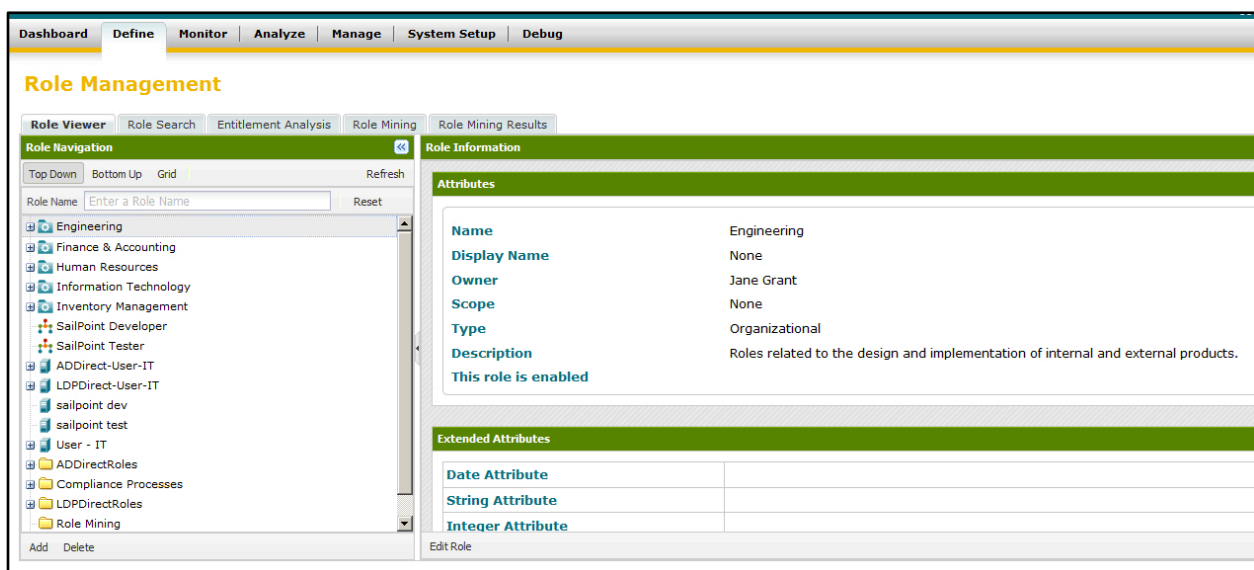
Some customers want to continue to model access to all their resources in a consistent manner using an account-centric model. For these customers, IdentityIQ provides Logical Applications. Logical Applications can be managed similarly to traditional applications, including how they are displayed in IdentityIQ's user interface (e.g. in application drop-down lists), the process by which Access Reviews are performed, and the way in which data is reported.



Name	Host	Type
Active_Directory	localhost	Delimited File Parsing Connector
ADDirectDemodata	schooner.test.sailpoint.com	Active Directory - Direct
AdminsApp	localhost	Delimited File Parsing Connector
Composite_ERP_Global_App_Users	localhost	Delimited File Parsing Connector
Composite_ERP_Global_DB	localhost	Delimited File Parsing Connector
Composite_ERP_Global_Platform	localhost	Delimited File Parsing Connector
ERP_Global		Logical
HR_Contractors	localhost	Delimited File Parsing Connector
HR_Employees	localhost	Delimited File Parsing Connector
NBA Active Directory	schooner.test.sailpoint.com	Active Directory
Oracle_DB_oasis	localhost	Delimited File Parsing Connector
Procurement_System	localhost	RACF

Figure 1: User Interface display of Logical Application

In other customer environments, application access has been separated from the application tier through the use of entitlements. This separation can facilitate the process by which organizations comply with regulatory requirements for access review and data transparency. Entitlements are the set of privileges that govern what an application user can do, often at a finer level of detail than simple account access. IdentityIQ's entitlement-centric Role Model provides a way of managing these entitlements so that they can be efficiently defined, assigned, reviewed, and revoked. When Roles are used, entitlements can be assigned through the Roles rather than being directly assigned to users.



**Role Management**

Role Navigation: Top Down | Bottom Up | Grid | Refresh

Role Name:  | Reset

**Role Information**

**Attributes**

Name	Engineering
Display Name	None
Owner	Jane Grant
Scope	None
Type	Organizational
Description	Roles related to the design and implementation of internal and external products.

**Extended Attributes**

Date Attribute	
String Attribute	
Integer Attribute	

Edit Role

Figure 2: Role Management User Interface

## Performance Impacts

When the number of Logical Applications exceeds about 25, performance is usually significantly better with Roles than with Logical Applications. With the performance improvements introduced on the 6.0 release, up to 500,000 Roles can be efficiently managed by IdentityIQ's Role Model . The performance considerations described below also may affect the decision process.

### Logical Applications Performance Considerations

Unlike traditional applications, Logical Applications cannot take advantage of optimized aggregation. For all other applications, the default behavior of the Account Aggregation task is to aggregate changed accounts only. A Logical account changes when a change occurs on one of the tier accounts. Because tracking individual tier account changes is very difficult, the aggregation process automatically refreshes every Logical account link, whether or not it has been changed since the last aggregation.

Moreover, the Identity Refresh task can run significantly more slowly with the option 'Refresh logical application links' when there are a large number of Logical Applications.

Finally, application account links generally consume more memory and processing cycles than do role assignments when accessing and updating identity objects. Like accounts on other application types, a Logical Application account is represented as a link on an identity cube. An account link contains a copy of the all the attributes and values configured for that application. As each new link is added, the size of the identity increases.

When a large identity object is accessed, the entire object, including all its links, is loaded into memory. Any change to the identity requires a database commit of the entire object. Operations on large identities (those with many accounts) can be slow, especially when generating and displaying certifications. In the following example, a Logical Application account link with one entitlement and one permission is represented as:

```
<Link
componentIds="2c9001213ed898ef013ed8a03676102e,2c9001213ed898ef013ed8a0142e0f19,2c9001
213ed898ef013ed8a0209b0fcc" created="1370479331227" entitlements="true"
id="2c90011f3f0bcbd1013f16ef079b0413" modified="1370479331310" identity="327">
  <ApplicationRef>
    <Reference class="sailpoint.object.Application"
id="2c9001213ed898ef013ed89ef5a70298" name="ERP_Global"/>
  </ApplicationRef>
  <Attributes>
    <Map>
      <entry key="directPermissions">
        <value>
          <List>
            <Permission rights="execute" target="SP_AppUserLogin">
              <Annotation>Annotation For Target: SP_AppUserLogin</Annotation>
            </Permission>
          </List>
        </value>
      </entry>
      <entry key="groupmbr">
        <value>
          <List>
            <String>FinancialSystems</String>
          </List>
        </value>
      </entry>
    </Map>
  </Attributes>
</Link>
```

```
        </List>
      </value>
    </entry>
  </Map>
</Attributes>
</Link>
```

In comparison, an assigned role is usually represented more concisely in an identity by a pointer to the role and its associated metadata:

```
<Bundles>
  <Reference class="sailpoint.object.Bundle" id="2c9001213ed898ef013ed89efd4302a6"
name="User - IT"/>
</Bundles>
<snip/>
<RoleMetadatas>
  <Reference class="sailpoint.object.RoleMetadata"
id="2c90010e3f77e48c013f8685c81600cd" name="User - IT"/>
</RoleMetadatas>
```

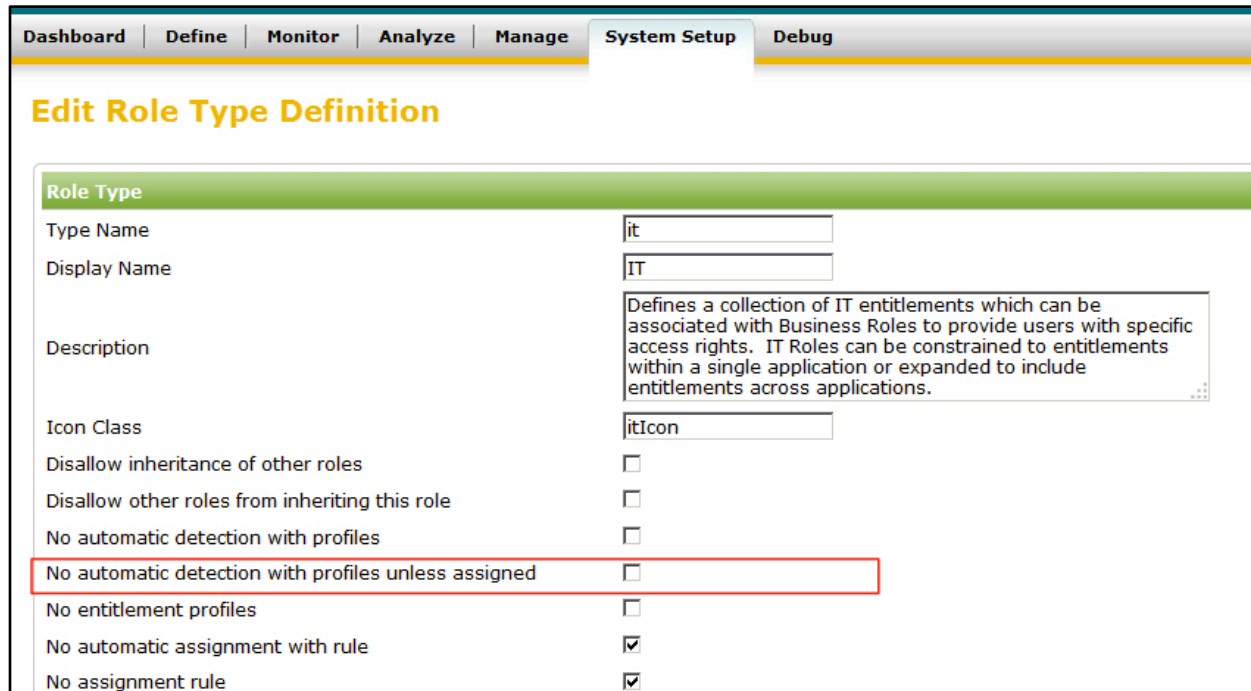
The bit size difference between these two representations can add up when processing high volumes of identities with high volumes of logical applications or roles.

## Role Performance Considerations

With the release of 6.0, IdentityIQ has been shown to perform well with up to 500,000 Roles in the Role Model. The 6.0 release introduced significant improvements to Role performance, especially to Entitlement Correlation, the process used to determine an identity's Roles and entitlements. Entitlement Correlation is invoked throughout the product including Identity Refresh, LCM requests, and certification generation. These improvements include more efficient caching and sharing of entitlement correlation data.

In addition, a new configuration option "No automatic detection with profiles unless assigned", which can be defined in **System Setup -> Role Configuration -> Edit Role Type**, will limit Role detection only to those Roles that are required or permitted by an assigned Role. When this option is not set, IdentityIQ must examine every role to determine if it should be added to an identity as a "detected" role. For customers with a large number of roles, this setting can have a significant impact on the time required to complete role detection.





Role Type	
Type Name	it
Display Name	IT
Description	Defines a collection of IT entitlements which can be associated with Business Roles to provide users with specific access rights. IT Roles can be constrained to entitlements within a single application or expanded to include entitlements across applications.
Icon Class	itIcon
Disallow inheritance of other roles	<input type="checkbox"/>
Disallow other roles from inheriting this role	<input type="checkbox"/>
No automatic detection with profiles	<input type="checkbox"/>
No automatic detection with profiles unless assigned	<input type="checkbox"/>
No entitlement profiles	<input type="checkbox"/>
No automatic assignment with rule	<input checked="" type="checkbox"/>
No assignment rule	<input checked="" type="checkbox"/>

Figure 3: 6.0 Configuration Option for Role Detection

## Ease of Configuration

In general, a level of technical expertise is required to create and maintain Logical Applications. Construction of a Logical Application typically requires an understanding of application schema. After the role model has been designed, a business user with minimal technical skills can usually create and maintain Roles using IdentityIQ's Role Management user interface

## Logical Applications

A Logical Application is defined based on a combination of attributes found on one or more existing IdentityIQ applications, referred to as "tiers". Unlike with other IdentityIQ applications, Logical Application accounts are not pulled from an external environment. Instead, Logical account links are created by examining identities, and looking for patterns that match the criteria defined for the tiers.

The most straightforward way to define these patterns is by entering "account matching" attributes on the 'Application Configuration' page.

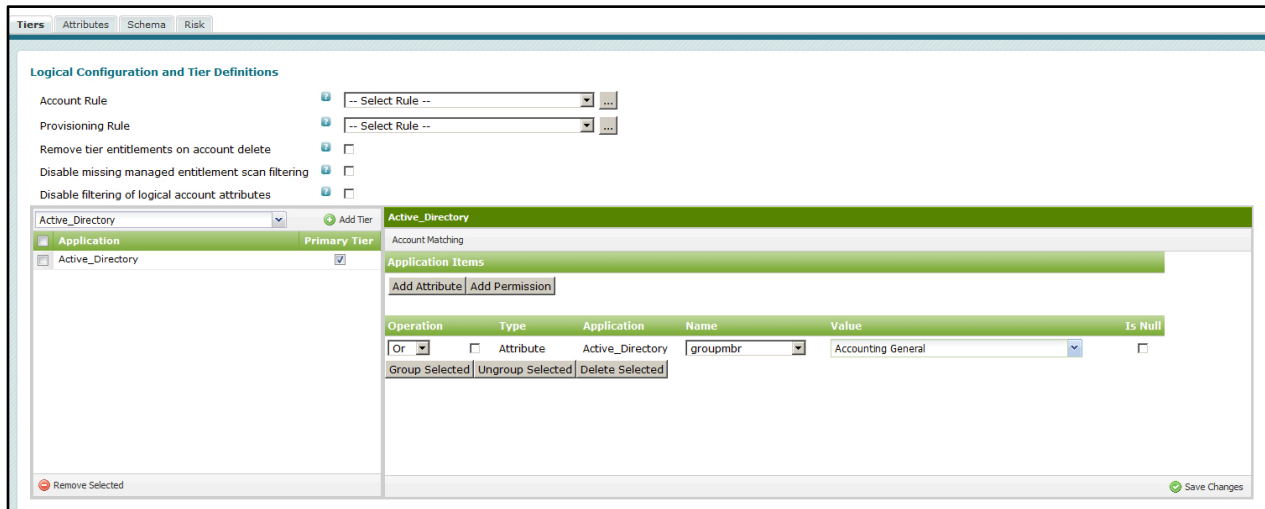


Figure 4: Logical Application Tier Account Matching Configuration

With tier account matching, a Logical Application account is created when:

- An account exists on every tier, and
- There is an exact match on attribute values

Alternately, an Account Rule can be written to customize tier matching for more complex use cases, including:

- Some subset of tier accounts exist, and/or
- A tier attribute that "starts with" or "contains" some specified value

Similarly, a Provisioning Rule can be used to customize the way that native tier accounts are updated. These rules are more flexible than the tier account matching configurations. But, they do add complexity, especially for deprovisioning.

Refer to "Native Identity Composite Account Rule" and "Example Composite Remediation Rule" in `$IIQ_HOME/WEB-INF/config/examplerules.xml` for examples of a Logical Application Account Rule and Logical Application Provisioning Rule.

Chapter 39 of the 6.1 "SailPoint IdentityIQ Direct Connectors Administration and Configuration Guide" contains detailed instructions for configuring the Logical Connector.

## Roles

Individual Roles can be created manually in the:

- **Define**->**Roles**->**Role Viewer** page, and
- **Monitor**->**Certifications**->**Access Review Detail** page when certifying entitlements

IdentityIQ's Role Mining process is a tool that can be used to efficiently automate the creation of both Business and IT Roles. Refer to Chapter 16 of the 6.1 "Sailpoint IdentityIQ Administration Guide" for complete information about setting up and using Role Management.

## Provisioning Flexibility

Roles are generally more flexible at provisioning than Logical Applications. A provisioning policy can be attached to individual roles, allowing for more granular provisioning control. In contrast, Logical account provisioning requests are converted to provisioning requests on the tiers, each of which may have a unique application provisioning policy.

## Logical Applications

Unlike Roles and other types of applications, Logical Applications cannot have provisioning policies. By default, provisioning operations on Logical accounts are performed on the tiers. For example, consider a Logical Application account with an entitlement value of 'Accounting' on the groupmbr attribute, created from the Account Matching tier definition. In the Logical Application's schema, 'groupmbr' is mapped to the 'memberOf' attribute on the tier account.

If this entitlement is revoked from the Logical account, the Provisioning Plan will initially be created as:

```
<ProvisioningPlan>
  <AccountRequest application="Logical Application" op="Modify">
    <AttributeRequest name="groupmbr" op="Remove" value="Accounting"/>
  </AccountRequest>
</ProvisioningPlan>
```

As the provisioning process progresses, the plan will be converted to:

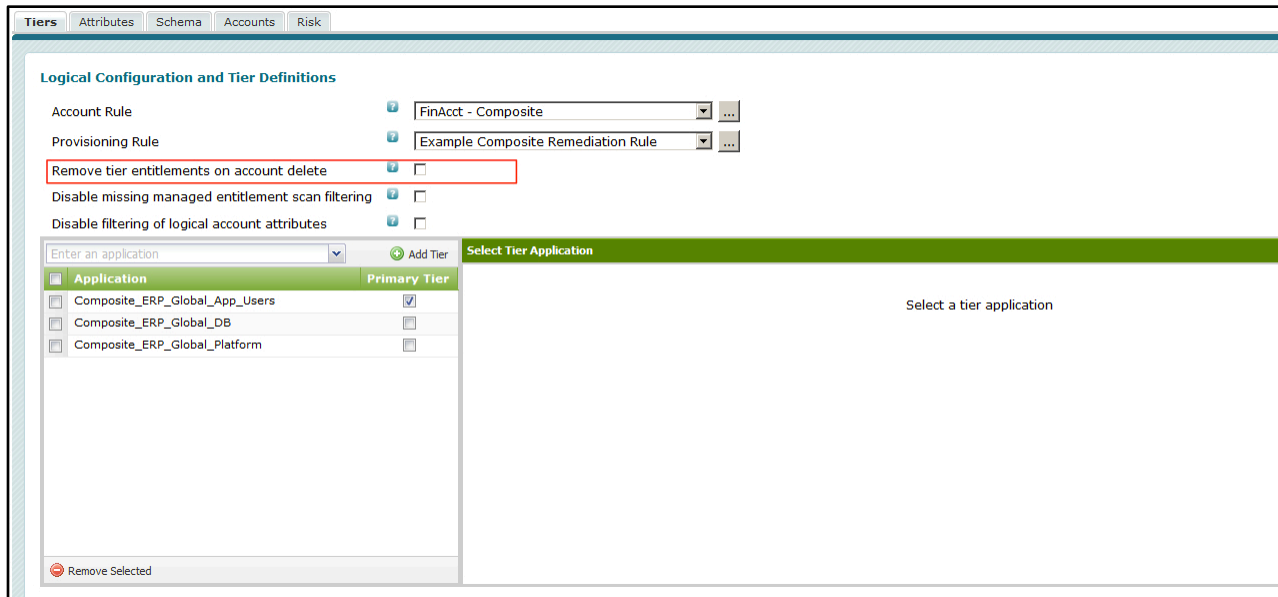
```
<ProvisioningPlan>
  <AccountRequest application="Tier Application" op="Modify">
    <AttributeRequest name="memberOf" op="Remove" value="Accounting"/>
  </AccountRequest>
</ProvisioningPlan>
```

The request will then be handled by the tier. After the entitlement is removed from the tier, it will be removed from the Logical account when the 'Identity Refresh' task with the option 'Refresh logical application links' is run. The Logical account will be deleted, if this is a required attribute for Account Matching.

Refresh the identity risk scorecards		<input type="checkbox"/>
Maintain identity histories		<input type="checkbox"/>
Refresh the group scorecards		<input type="checkbox"/>
Clean up groups definitions that are no longer referenced		<input type="checkbox"/>
Check active policies		<input type="checkbox"/>
Keep previous violations		<input type="checkbox"/>
A comma separated list of specific policy names. When set this overrides the default policies.		<input type="text"/>
Refresh assigned scope		<input type="checkbox"/>
Disable auto creation of scopes		<input type="checkbox"/>
Mark dormant scopes after refresh		<input type="checkbox"/>
Refresh continuous certifications		<input type="checkbox"/>
Process events		<input type="checkbox"/>
Refresh logical application links		<input checked="" type="checkbox"/>
Promote managed attributes		<input type="checkbox"/>
Number of Refresh Threads		<input type="text"/>
Always launch the workflow (even if the usual triggers don't apply)		<input type="checkbox"/>
Enable the generation of work items for unmanaged parts of the provisioning plan.		<input type="checkbox"/>

Figure 5: Identity Refresh Option to Refresh Logical Links

The Logical Application configuration setting 'Remove tier entitlements on account delete' controls the removal of entitlements from tier accounts when a Logical account is deleted.



**Figure 6: Remove Tier Entitlement Configuration for Logical Application**

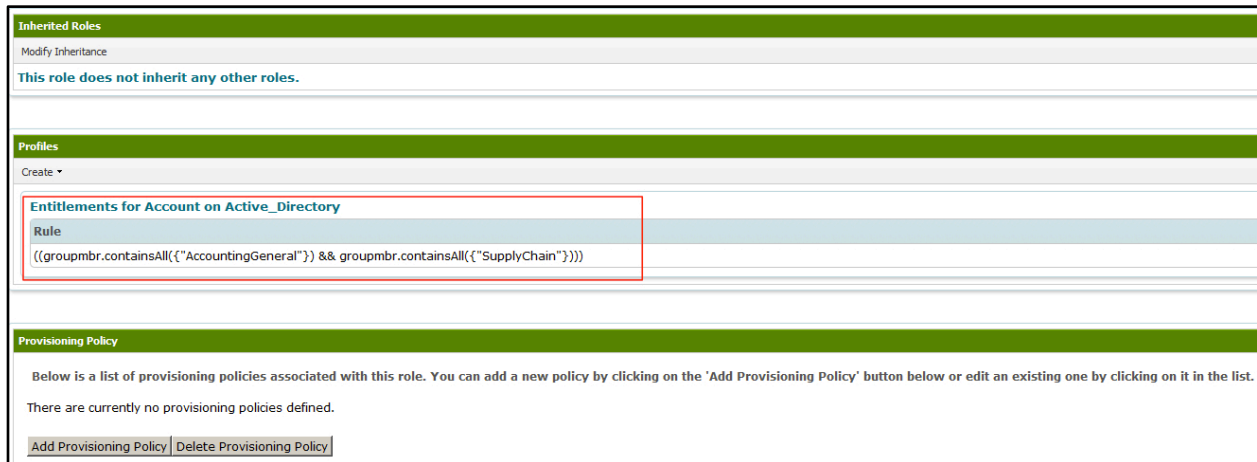
The default behavior for tier account provisioning can be customized by assigning a Provisioning Rule to the Logical Application. When an Account Rule is used to customize tier matching, a Provisioning Rule is usually needed to specify the way that native tier accounts should be updated during provisioning. For example, using the screenshot above as an example, an Account Rule may specify that a Logical Account should be created if an account match is found on:

- Composite\_ERP\_Global\_App\_Users, and
- either Composite\_ERP\_Global\_DB or Composite\_ERP\_Global\_Platform

A Provisioning Rule could be written to "deconstruct" the custom updates performed for this tier structure, when the Logical account is updated or revoked. Although not required by IdentityIQ, Best Practices dictate that if a logical account has been created using an Account Rule, the inverse of the Account Rule instructions should be used to deprovision the account via a Provisioning Rule. For the "subdivide" use case, deprovisioning is typically fairly simple. Deprovisioning the "composite" use case can be complex.

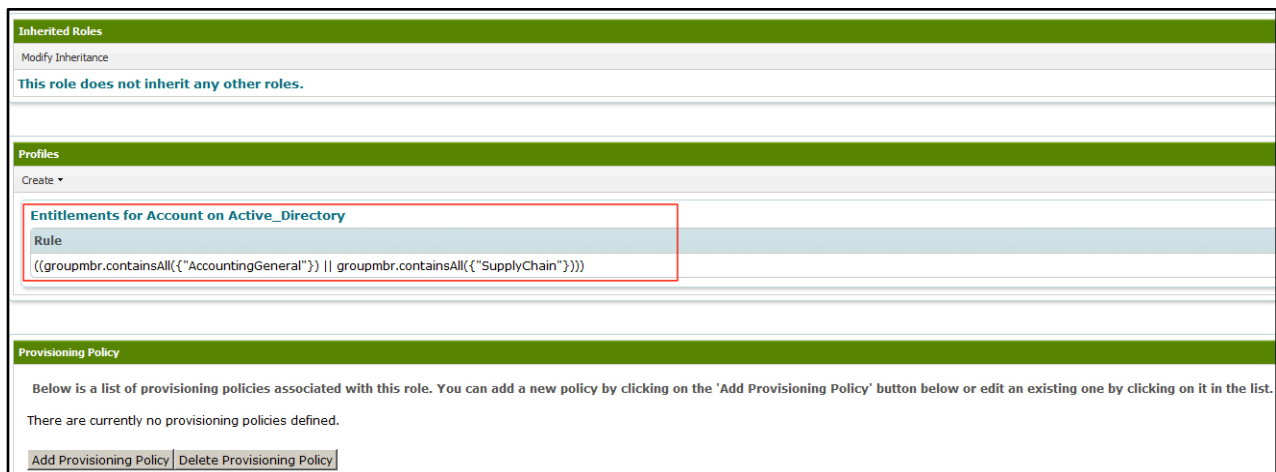
## Roles

A role profile can define how the encapsulated entitlements are provisioned and deprovisioned. When the role profile has a single field in its filter, or when multiple fields are "AND'ed" together, IdentityIQ can easily analyze the role profile and provision entitlements to match the profile. For example, to satisfy the following profile, an identity must have the values "AccountingGeneral" and "SupplyChain" in its groupmbr attribute. When this role is provisioned, a request for both attribute values will be included in the provisioning plan.



**Figure 7: Role Profile with AND'ed entitlements**

Provisioning can be ambiguous, though, when a role profile contains "OR'ed" terms, for example "AccountingGeneral" or "SupplyChain" in its groupmbr attribute:

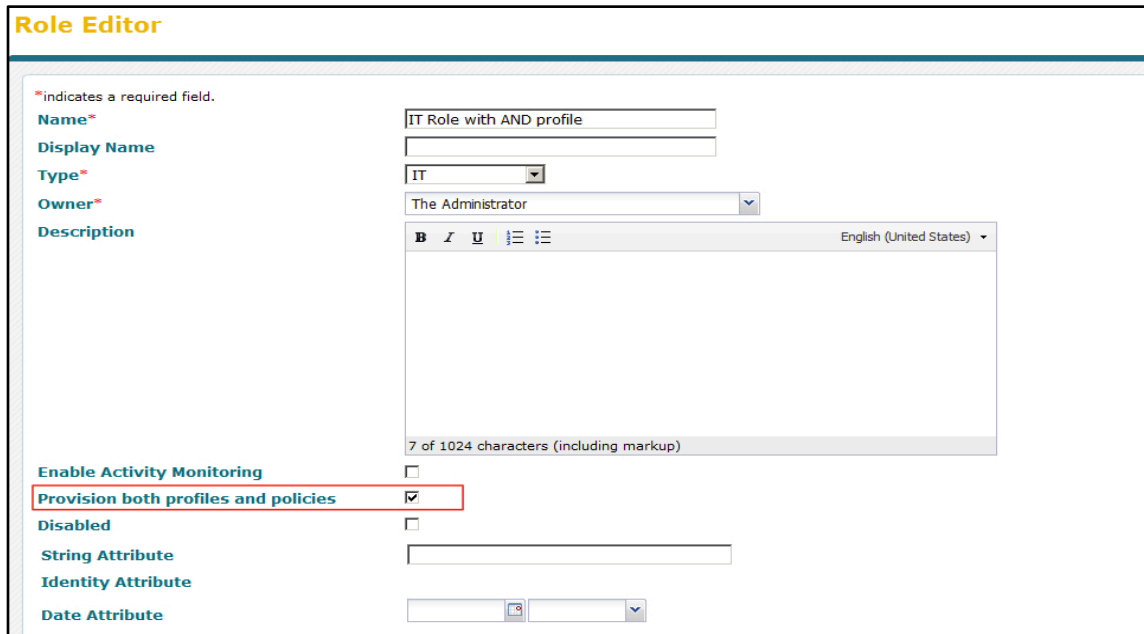


**Figure 8: Role Profile with OR'ed entitlements**

With "OR'ed" terms, IdentityIQ provisions and deprovisions the first attribute value that it finds. In this example, there will be a single attribute request for either "AccountingGeneral" or " SupplyChain ".

IdentityIQ inverts the profile when the Role is deprovisioned.

A Provisioning Policy can be used to override or supplement the role profile. Prior to the 6.0 release, if a Provisioning Policy was defined for a Role, the role profile was not used for provisioning. The 6.0 release added the configuration option "Provision both profiles and policies" to the Role Editor.



**Role Editor**

\* indicates a required field.

**Name\*** IT Role with AND profile

**Display Name**

**Type\*** IT

**Owner\*** The Administrator

**Description**

7 of 1024 characters (including markup)

**Enable Activity Monitoring**

**Provision both profiles and policies**

**Disabled**

**String Attribute**

**Identity Attribute**

**Date Attribute**

Figure 9: Role Configuration Option to Provision both profiles and policies

When this option is checked, the Role profile will supplement the Provisioning Policy when the Role is provisioned. Without this option, it may be necessary to duplicate the profile attribute rules in the Provisioning Policy.

Unlike Applications, which have separate Provisioning Policies for creates, updates, and deletes, a single Provisioning Policy is available for Roles.

## Other Resources

These additional documents, which can be found on Compass, provide more detailed information about how to configure and use Logical Applications and Roles in IdentityIQ.

- Role Management in IdentityIQ.pdf
- 6\_1\_IdentityIQ\_Direct\_Connectors\_Admin\_and\_Config\_Guide.pdf (for instructions on configuring Logical Applications)
- 6\_1\_IdentityIQ\_Administration\_Guide.pdf (for instructions on configuring Roles)

## Document Revision History

Revision Date	Written/Edited By	Comments
July, 2013	Nena Hunt	Initial Creation; current IdentityIQ Version: 6.1