Provisioning with IdentityIQ

IdentityIQ Version: 5.5

The information in this white paper has been merged into the IdentityIQ Administration Guide. Future updates to this content will be made only in that document; this white paper will not be updated for future releases.

This document discusses the flow of data from initial request in IdentityIQ through provisioning of accounts and entitlements in the source applications.

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.

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.

Table of Contents

Overview

IdentityIQ's provisioning capabilities help companies manage system access for their personnel. Modifications to Identities' access or Entitlements requested in IdentityIQ can, in many cases, be automatically reflected in the native applications to which that access applies. Provisioning requests can be created and processed in several ways in IdentityIQ, depending on the needs and configuration of the installation.

At a high level, provisioning requests are processed as follows:

- The provisioning request is made through one of several mechanisms.
- The request is created as a Provisioning Plan.
- The Provisioning Plan is evaluated and compiled by the Provisioning Broker. Often this involves splitting the original plan out in to several partitioned plans that each address a single application. This also includes identifying how the request will be processed: by an Integration Config, by a Provisioning Engine read-write connector, or manually through an internal Work Item in IdentityIQ.
- Each partitioned Provisioning Plan is passed to the appropriate handler.
- In the case of Integration Config or read-write connectors, the change is written to the destination system. In the case of Work Items, a Work Item is created and assigned to an Identity who is responsible for manually processing the request into the target system.

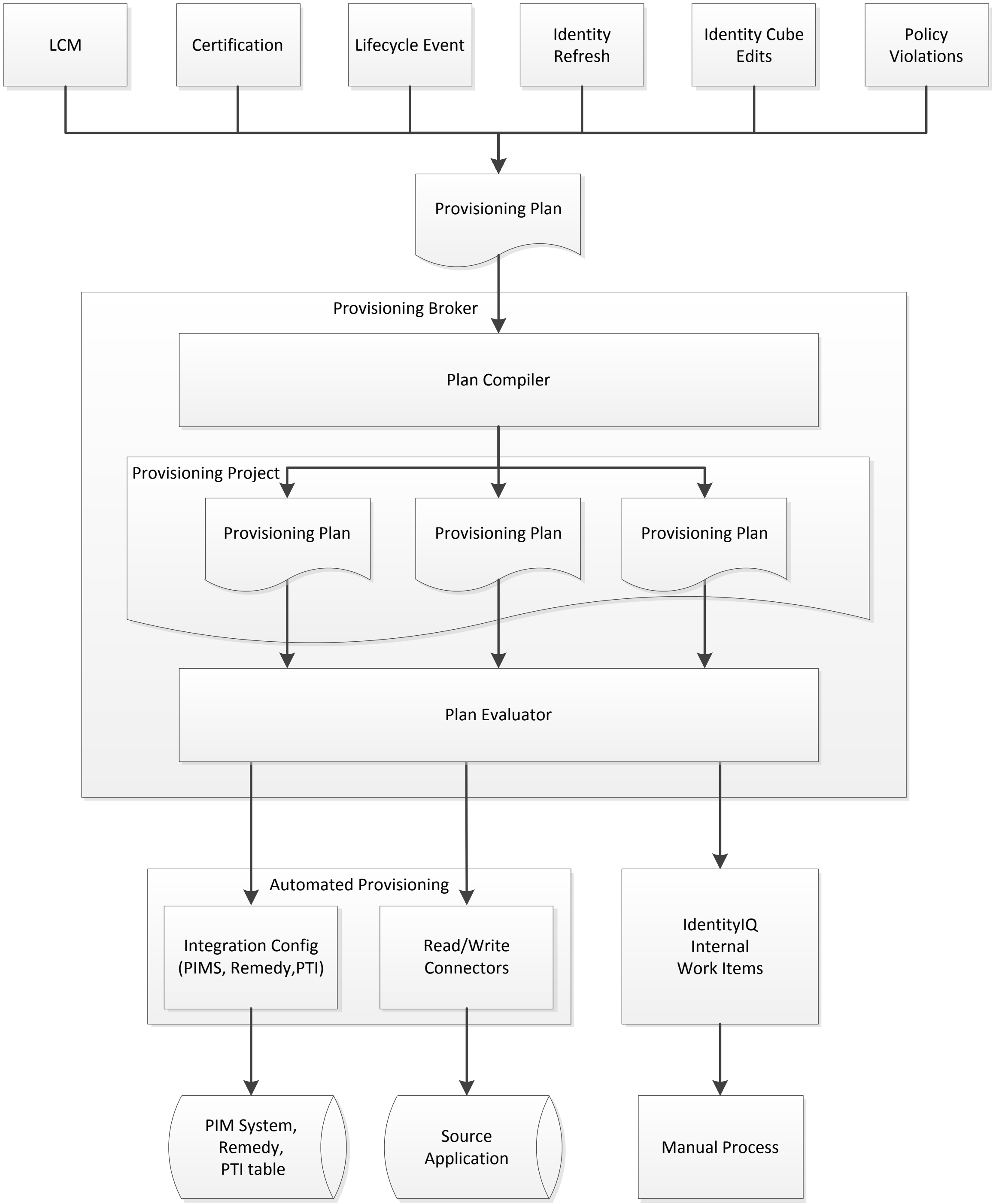


Figure 1: Provisioning Overview

This document describes the provisioning procedures in IdentityIQ in detail. It begins by describing IdentityIQ's facilities for making provisioning requests. It then traces the flow of the Provisioning Plan through its evaluation and preparation for being processed into the appropriate native system. Finally, it describes how the provisioning actions are confirmed and marked on the Identity Cube, depending on the mechanisms involved. Included throughout are the IdentityIQ tasks, workflows, and rules that operate on the data as it moves through the process.

Recording Provisioning Requests

Provisioning requests can be created in IdentityIQ through any of these actions or activities:

- Certification remediations and provisioning requests
- Policy violation remediations
- Identity Refresh-driven Role assignments
- Event-driven provisioning through Lifecycle Event tasks/workflows
- Lifecycle Manager (LCM) requests
- Direct updates to the Identity Cube

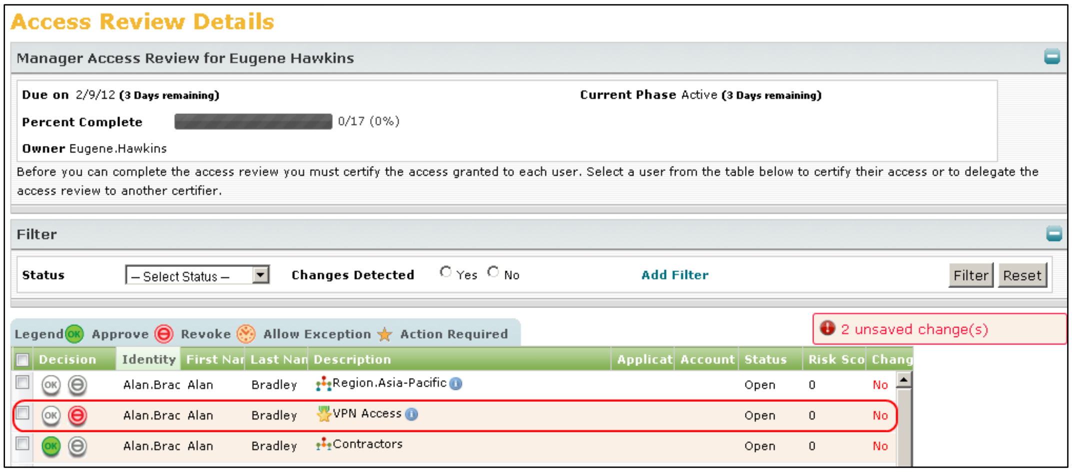
All provisioning requests result in the creation of a Provisioning Plan that can be analyzed and processed by the Provisioning Broker. In most cases (all but Certification- and Policy-Violation-generated requests), they also create a Workflow Case that manages the processing of the provisioning request according to a defined Workflow. (See Processing Provisioning Requests for more details.)

Certifications

During a Certification Access Review, certifiers review the system Entitlements granted to sets of Identities. Access can be approved or revoked for an Identity during this review process. Revocations result in remediations in the source system to remove the inappropriate access from the Identity's account. In some cases, the certifier may be notified that an Identity is missing some required system access which the certifier may request for the Identity, generating a provisioning request for that access.

Certification Remediation

When an Identity's access to a system is deemed to be inappropriate for their job function, the certifier can revoke the Entitlement through the Certification Access Review. This creates a (remediation) provisioning request in IdentityIQ to remove that access from the source application.



Access Review Details

Manager Access Review for Eugene Hawkins

Due on 2/9/12 **(3 Days remaining)** **Current Phase** Active **(3 Days remaining)**

Percent Complete 0/17 (0%)

Owner Eugene.Hawkins

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

Status – Select Status – **Changes Detected** ○ Yes ○ No **Add Filter** Filter Reset

Legend OK Approve ⊖ Revoke Allow Exception ★ Action Required

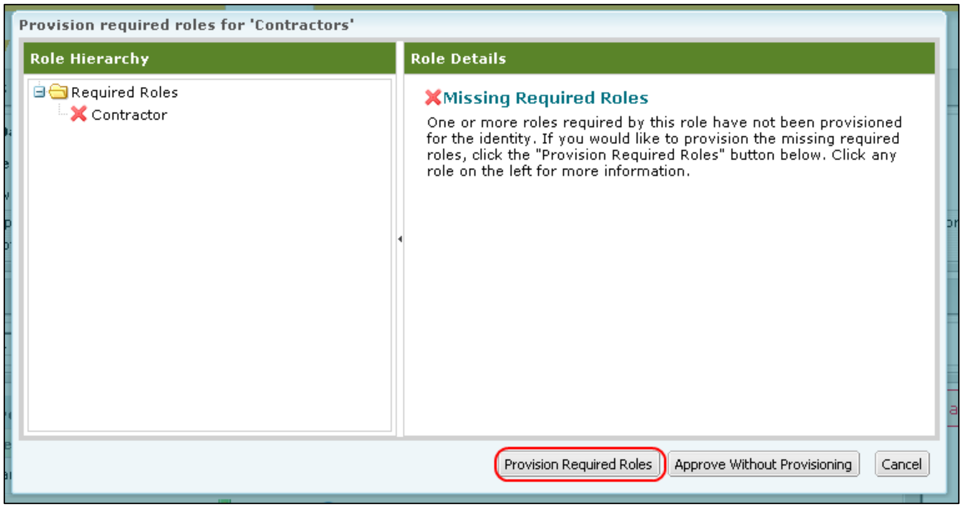
2 unsaved change(s)

□	Decision	Identity	First Nar	Last Nan	Description	Applicat	Account	Status	Risk Sco	Chang
□	OK ⊖	Alan.Brac	Alan	Bradley	Region.Asia-Pacific			Open	0	No
□	OK ⊖	Alan.Brac	Alan	Bradley	VPN Access			Open	0	No
□	OK ⊖	Alan.Brac	Alan	Bradley	Contractors			Open	0	No

Figure 2: Revocation request from Certification

Provisioning through Certifications

When a Business Role is approved for an Identity that includes Required (IT) Roles the Identity does not currently have, the certifier may be prompted to choose whether the missing Role(s) should be provisioned for the Identity or whether the Business Role should be approved without provisioning the missing Role(s). If the certifier elects to provision the missing Roles, a provisioning request is created.



Provision required roles for 'Contractors'

Role Hierarchy

- Required Roles
  - Contractor

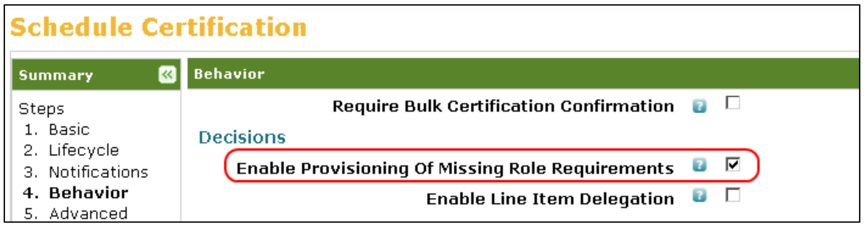
Role Details

Missing Required Roles

One or more roles required by this role have not been provisioned for the identity. If you would like to provision the missing required roles, click the "Provision Required Roles" button below. Click any role on the left for more information.

Figure 3: Optional Provisioning of Missing Required Roles

NOTE: This provisioning option is only presented during the Access Review if the option “Enable Provisioning of Missing Role Requirements” is selected in the Certification specification.



Schedule Certification

Summary

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

Behavior

Require Bulk Certification Confirmation □

Decisions

Enable Provisioning Of Missing Role Requirements ☑

Enable Line Item Delegation □

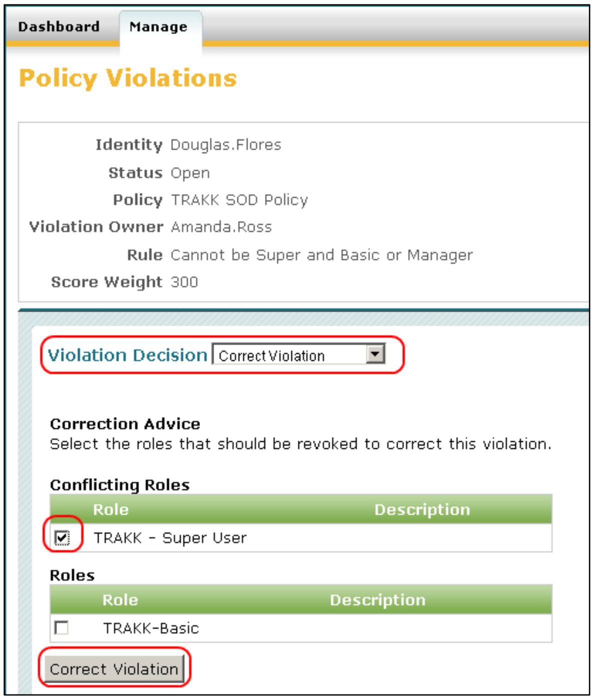
Figure 4: Provisioning Option in Certification Specification

NOTE: Except in Certifications where revocations are processed immediately (continuous certifications and certifications with the Process Revokes Immediately setting selected), all revocations and provisioning requests from a specific access review are combined into a single provisioning plan and processed together.

Policy-Violation Remediation

Policies defined in IdentityIQ allow the system to evaluate an Identity’s access or activities and report inconsistencies with the company’s stated policies. The violations are reported to the violation owner (often the Identity’s manager or the appropriate application owner) who can act upon them by permitting an exception or by initiating a remediation request. For example, when a manager evaluates an Identity’s Separation of Duties violations and determines that one of the Identity’s accesses should be removed, he can request revocation of the invalid access.

Policy Violation remediation requests can be created from the policy owner's **Manage** -> **Policy Violations** page or from a Certification on which the violation is noted.



Policy Violations

Identity	Douglas.Flores
Status	Open
Policy	TRAKK SOD Policy
Violation Owner	Amanda.Ross
Rule	Cannot be Super and Basic or Manager
Score Weight	300

Violation Decision: Correct Violation

Correction Advice
Select the roles that should be revoked to correct this violation.

Conflicting Roles

	Role	Description
☑	TRAKK - Super User	

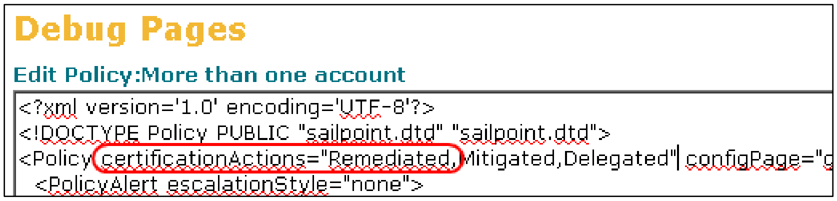
Roles

	Role	Description
□	TRAKK-Basic	

Figure 5: Policy Violation Remediation -- Correcting Violation

Only remediations for Role or Entitlement Separation of Duties (SOD) violations generate a provisioning request to revoke the invalid access. Other types of policy violations do not have clear remediation actions associated and therefore cannot generate provisioning requests to complete the remediation.

By default, non-SOD policy violations cannot be remediated through a certification or on the policy violation window. However, the XML for any policy can be edited to include "remediated" as one of its certificationActions values, enabling certification remediation on that policy type.



```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Policy PUBLIC "sailpoint.dtd" "sailpoint.dtd">
<Policy certificationActions="Remediated,Mitigated,Delegated" configPage="g
  <PolicyAlert escalationStyle="none">
```

Figure 6: Non-SOD Policy Configured for Remediation

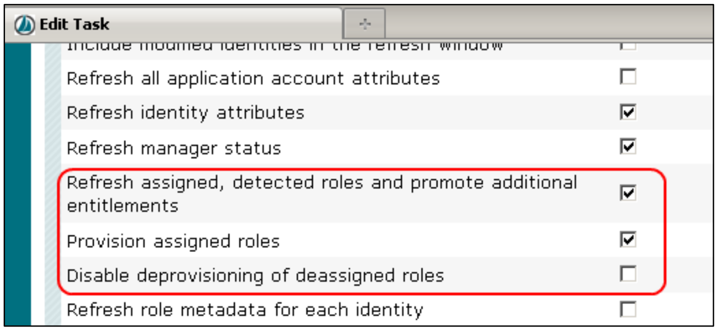
When non-SOD violations have been configured to be remediate-able, selecting the remediation option for the violation in a certification automatically creates a Work Item to inform the appropriate party of the need to correct the violation. A provisioning request is not created to process these violations.

Identity-Refresh-Driven Assignments

Certain options on an Identity Refresh task can cause provisioning requests to be generated for Identities.

The **Refresh assigned, detected roles and promote additional entitlements** option runs the Roles' defined Assignment Rules and examines Role detection profiles to update the Identity's Assigned and Detected role lists. This option does not provision access in external systems, but it does create provisioning requests to IdentityIQ to add Roles to those Identity Cubes.

The **Provision assigned roles** option generates provisioning requests to ensure that the Entitlements required for a newly assigned Role's "Required Roles" are added for the Identity. This option creates provisioning requests that apply to external applications, but only when the role is first assigned. If an Identity has existing assigned Roles whose Required Roles change, this option does provision the new Required Roles' Entitlements.



Include modified identities in the refresh window ☐
Refresh all application account attributes ☐
Refresh identity attributes ☑
Refresh manager status ☑
Refresh assigned, detected roles and promote additional entitlements ☑
Provision assigned roles ☑
Disable deprovisioning of deassigned roles ☐
Refresh role metadata for each identity ☐

Figure 7: Provisioning-Related Identity Refresh Task Options

NOTE: By default, the Entitlements associated with a Role are deprovisioned when the role is removed from an Identity. The **Disable deprovisioning of deassigned roles** option overrides that default and leaves the Entitlements intact for the Identity while the Role is removed.

Lifecycle Manager Requests

Lifecycle Manager (LCM) is a separately licensed portion of the IdentityIQ product that is designed for managing Entitlements through provisioning requests. Depending on the LCM configuration and the user's manager status, requests can be made through LCM on the user's own behalf or on behalf of other Identities. In a typical configuration, managers can make requests on behalf of their direct reports, and any user can make requests on their own behalf.

When LCM is enabled, the LCM toolbar appears (by default) at the top of each user's IdentityIQ Dashboard view. It offers the options of requesting Roles or Entitlements for Identities, managing accounts, managing passwords, and creating, editing, or viewing Identities. The set of Identities for which these actions can be taken depends on the individual user's authority and the LCM configuration. The self-service (Request For Me) options, of course, do not include Create Identity.

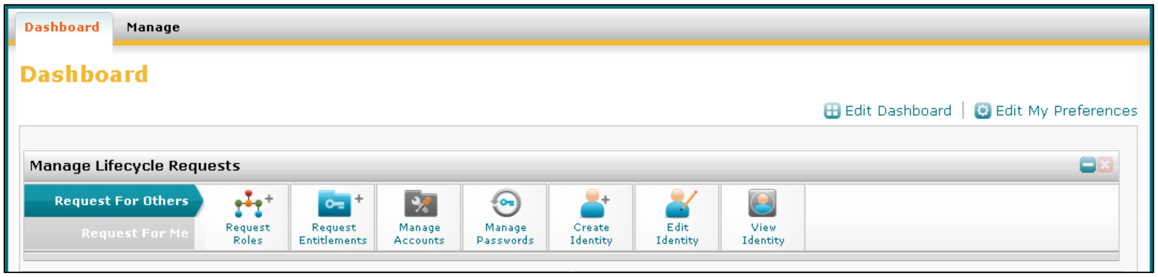
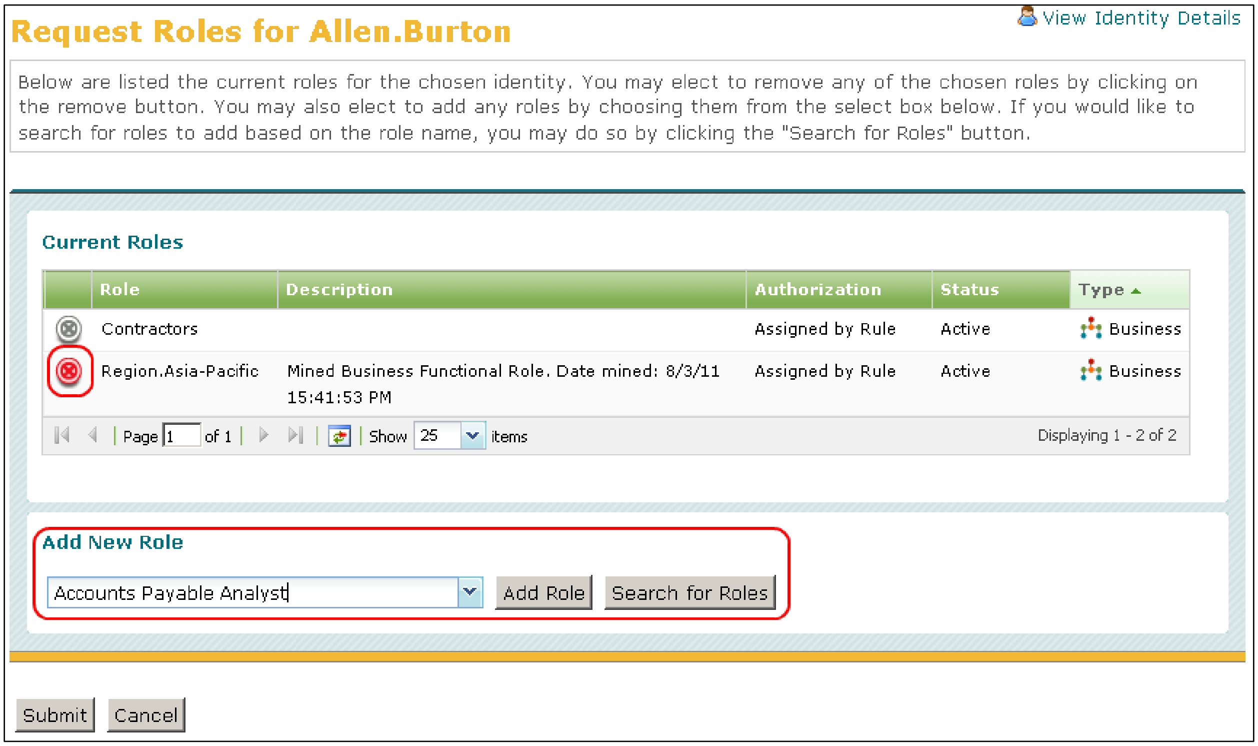


Figure 8: LCM Dashboard

Request Roles

Roles requested for an Identity through LCM's Request Roles feature generate provisioning requests to add the appropriate Role to the specified Identity or Identities. This includes provisioning the Entitlements associated with the Role's "Required Roles" (and "Permitted Roles", if added to the request when prompted).

Additionally, an Identity's existing Roles can be removed through this window, generating a remediation provisioning request to remove the Role(s) from the selected Identity Cube(s).


Request Roles for Allen.Burton

View Identity Details

Below are listed the current roles for the chosen identity. You may elect to remove any of the chosen roles by clicking on the remove button. You may also elect to add any roles by choosing them from the select box below. If you would like to search for roles to add based on the role name, you may do so by clicking the "Search for Roles" button.

Current Roles

	Role	Description	Authorization	Status	Type ▲
⊗	Contractors		Assigned by Rule	Active	Business
⊗	Region.Asia-Pacific	Mined Business Functional Role. Date mined: 8/3/11 15:41:53 PM	Assigned by Rule	Active	Business

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

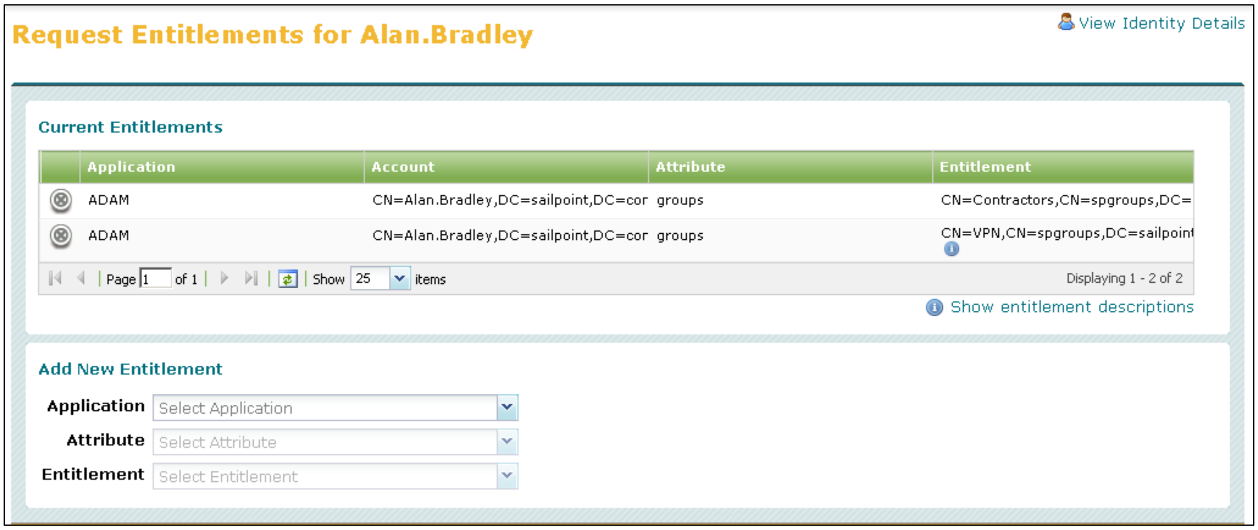
Add New Role

Accounts Payable Analyst

Figure 9: Removing and Adding Roles through LCM

Request Entitlements

Any Entitlement request added through LCM's **Request Entitlements** option generates a provisioning request to add the Entitlement to the specified Identity. An Identity's current Entitlements can also be revoked on the Request Entitlements window, generating provisioning requests to remove the access from the source application(s).



Request Entitlements for Alan.Bradley

View Identity Details

Current Entitlements

	Application	Account	Attribute	Entitlement
⊗	ADAM	CN=Alan.Bradley,DC=sailpoint,DC=cor	groups	CN=Contractors,CN=spgroups,DC=
⊗	ADAM	CN=Alan.Bradley,DC=sailpoint,DC=cor	groups	CN=VPN,CN=spgroups,DC=sailpoint

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

Show entitlement descriptions

Add New Entitlement

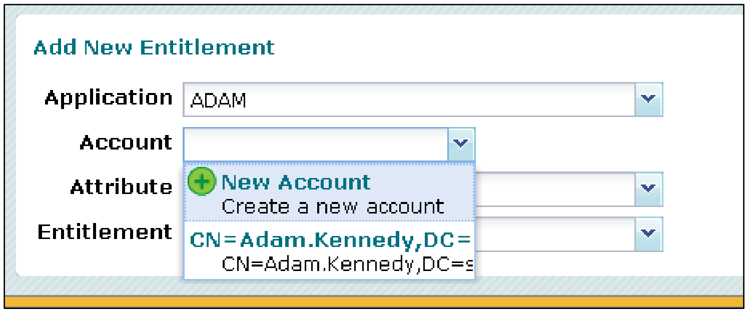
Application: Select Application

Attribute: Select Attribute

Entitlement: Select Entitlement

Figure 10: Request Entitlements Window

By default, when a new Entitlement is requested on an application where the user already has an account, that Entitlement will be added to the existing account. In some circumstances, it may be permissible and desirable to create a separate account for certain Entitlements. The ability to create multiple accounts for a single Identity on an application is controlled by the “Applications that support additional account requests” list on the **System Setup** -> **Lifecycle Manager Configuration** -> **Additional Options** page. When an application included in that list is selected as the **Application** in the **Add New Entitlement** section, an **Account** selection option appears that allows the requester to create a new account or add the Entitlement to an existing account held by the Identity.



Add New Entitlement

Application: ADAM

Account:

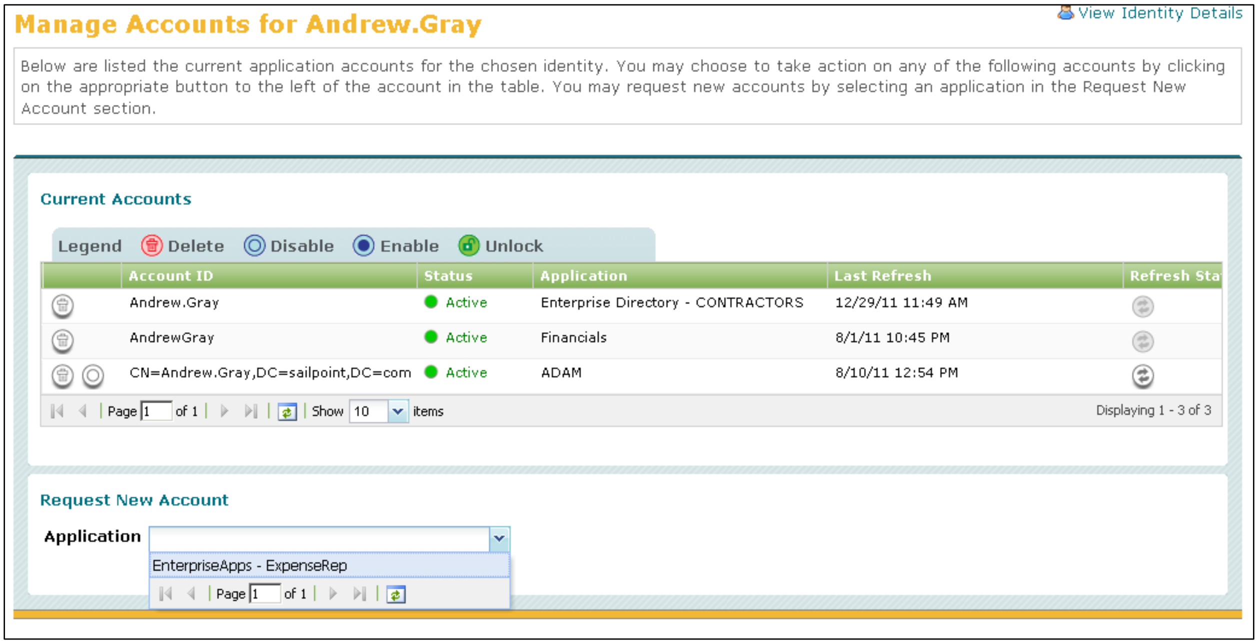
Attribute:

Entitlement:

Figure 11: Account Selection Option for New Entitlement

Manage Accounts

In the **Manage Accounts** window, accounts on additional applications can be requested and existing accounts can be revoked or disabled, all of which generate provisioning requests.



Manage Accounts for Andrew.Gray

Below are listed the current application accounts for the chosen identity. You may choose to take action on any of the following accounts by clicking on the appropriate button to the left of the account in the table. You may request new accounts by selecting an application in the Request New Account section.

Current Accounts

Legend: Delete, Disable, Enable, Unlock

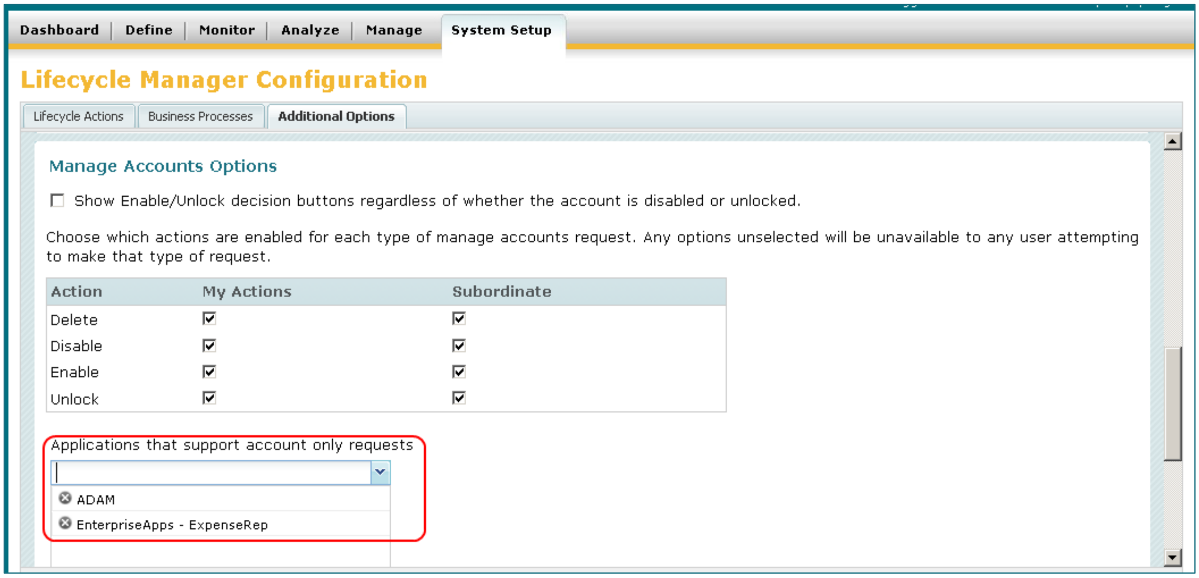
	Account ID	Status	Application	Last Refresh	Refresh Sta
	Andrew.Gray	● Active	Enterprise Directory - CONTRACTORS	12/29/11 11:49 AM	
	AndrewGray	● Active	Financials	8/1/11 10:45 PM	
	CN=Andrew.Gray,DC=sailpoint,DC=com	● Active	ADAM	8/10/11 12:54 PM	

Request New Account

Application: EnterpriseApps - ExpenseRep

Figure 12: Manage Accounts Window

NOTE: Applications appear in the **Request New Account** - **Application** list based on the Lifecycle Manager configuration. This list is populated with applications that are included in the “Applications that support account only requests” list in the **Manage Accounts Options** section of the **System Setup** -> **Lifecycle Manager Configuration** -> **Additional Options** tab.



Lifecycle Manager Configuration

Manage Accounts Options

□ Show Enable/Unlock decision buttons regardless of whether the account is disabled or unlocked.

Choose which actions are enabled for each type of manage accounts request. Any options unselected will be unavailable to any user attempting to make that type of request.

Action	My Actions	Subordinate
Delete	☑	☑
Disable	☑	☑
Enable	☑	☑
Unlock	☑	☑

Applications that support account only requests

- ADAM
- EnterpriseApps - ExpenseRep

Figure 13: Manage Account options configuration

Other LCM Options

The **Create Identity** and **Edit Identity** functionality could trigger a Lifecycle Event-driven provisioning request (see next section) but do not, in themselves, contain any provisioning-related actions. Likewise, **Manage Passwords** and **View Identities** do not involve provisioning-related functionality.

Lifecycle Event-Driven Provisioning

With LCM enabled, Lifecycle Events can be configured in IdentityIQ to represent activities that happen in the normal course of a person's employment at a company: events like joining the company, changing departments/managers, leaving the company. These events are also referred to by the shorthand terms: Joiner, Mover, Leaver.

When LCM is enabled, IdentityIQ contains four pre-defined Lifecycle Events.

- Joiner
- Leaver
- Manager Transfer
- Reinstate

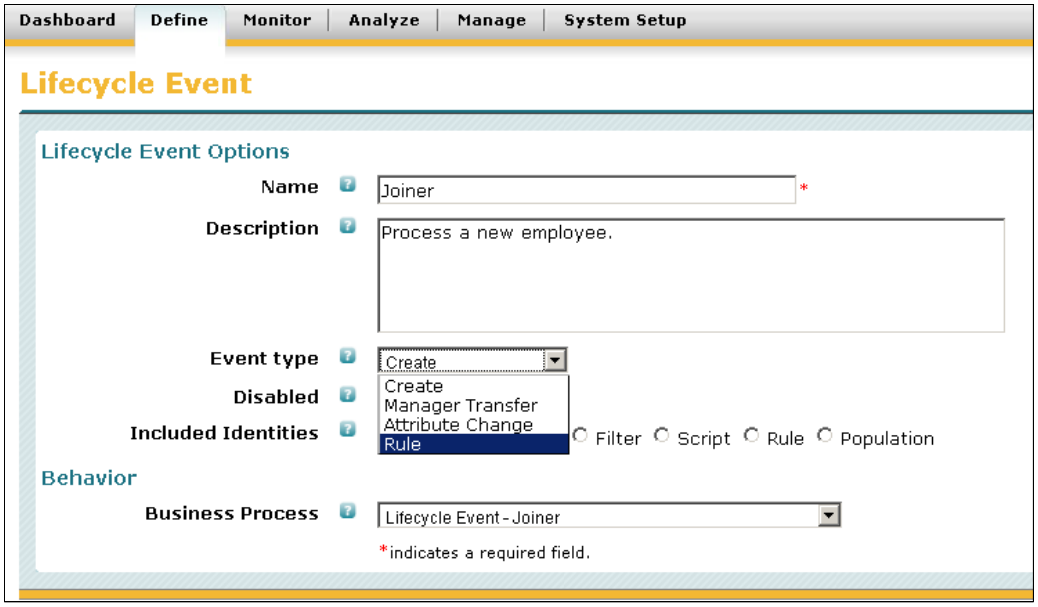
All of these are disabled by default and must be enabled before they will be triggered. Lifecycle Events are triggered by specific changes to an Identity – creation, manager transfer, attribute change, or more complex changes detected by an IdentityTrigger Rule. They invoke Business Processes, or Workflows, which may contain provisioning actions, if desired.

NOTE: The terms Business Process and Workflow are synonymous. The IdentityIQ user interface refers to them as Business Processes -- the term most often used by business managers. Behind the scenes, in the IdentityIQ object model and XML, they are called Workflows; they control the flow of data through the required processing.

The pre-defined Lifecycle Events function, by default, as shown in the table below.

Lifecycle Event	**Trigger**	**Business Process Invoked**
Joiner	Identity Creation	Lifecycle Event – Joiner
Leaver	Attribute Change: "Inactive" attribute change from false to true	Lifecycle Event – Leaver
Manager Transfer	Manager Change	Lifecycle Event – Manager Transfer
Reinstate	Attribute Change: "Inactive" attribute change from true to false	Lifecycle Event – Reinstate

The pre-defined events can be edited, or new Lifecycle Events can be created, through the **Define** -> **Lifecycle Event** window.



Lifecycle Event

Lifecycle Event Options

Name: Joiner *

Description: Process a new employee.

Event type: Create

Create
Manager Transfer
Attribute Change
Rule

Disabled

Included Identities: ○ Filter ○ Script ○ Rule ○ Population

Behavior

Business Process: Lifecycle Event - Joiner

*indicates a required field.

Figure 14: Defining/Editing Lifecycle Events

The default actions of each of the Business Process invoked by the pre-defined Lifecycle Events are noted below.

- **Lifecycle Event – Joiner**: prints Identity’s name to sysout; no actions taken on Identity itself (commonly modified to provision birthright access for Identities)
- **Lifecycle Event – Leaver**: creates and executes a ProvisioningPlan to disable all access held by the leaving Identity
- **Lifecycle Event – Manager Transfer**: prints names of old and new manager to sysout; no actions taken on Identity itself or Entitlements (commonly modified to generate a Certification for the new manager to review Identity’s access; may also provision birthright access identified for members of new manager’s group)
- **Lifecycle Event – Reinstate**: creates and executes a ProvisioningPlan to enable all (previously disabled) access held by the returning Identity

These actions can be modified through the Process Designer tab on the **Define** -> **Business Process** page or through the XML for the Workflow (accessible through the IdentityIQ Debug pages).

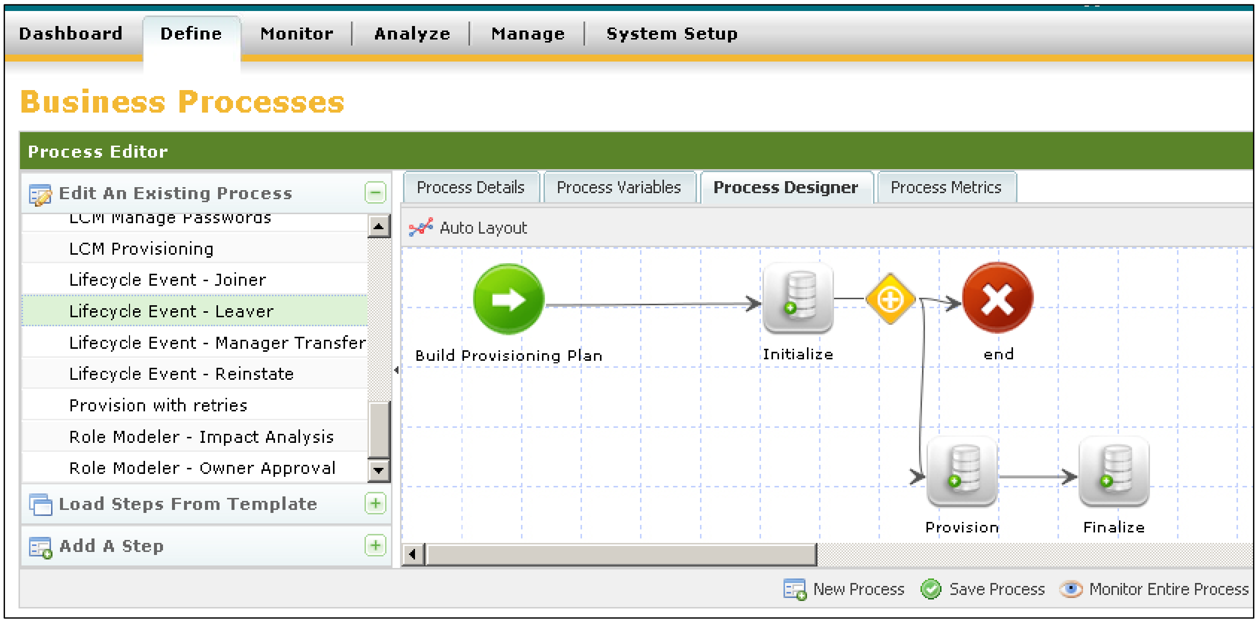
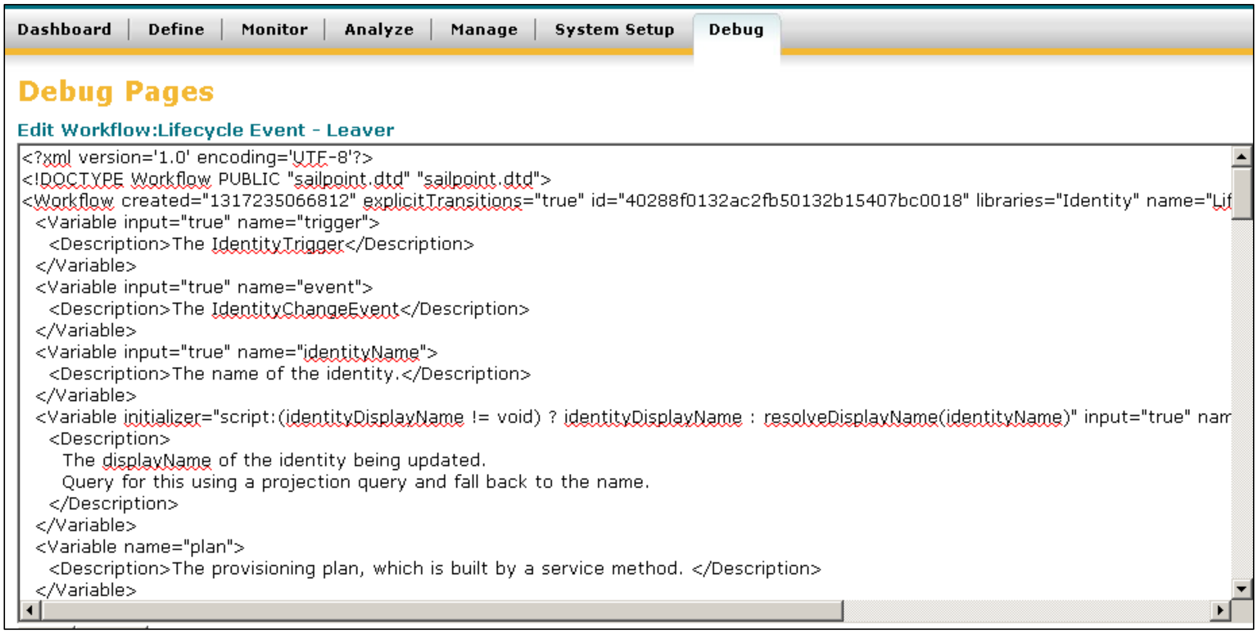


Figure 15: Edit Business Process through Process Designer tab



Edit Workflow:Lifecycle Event - Leaver

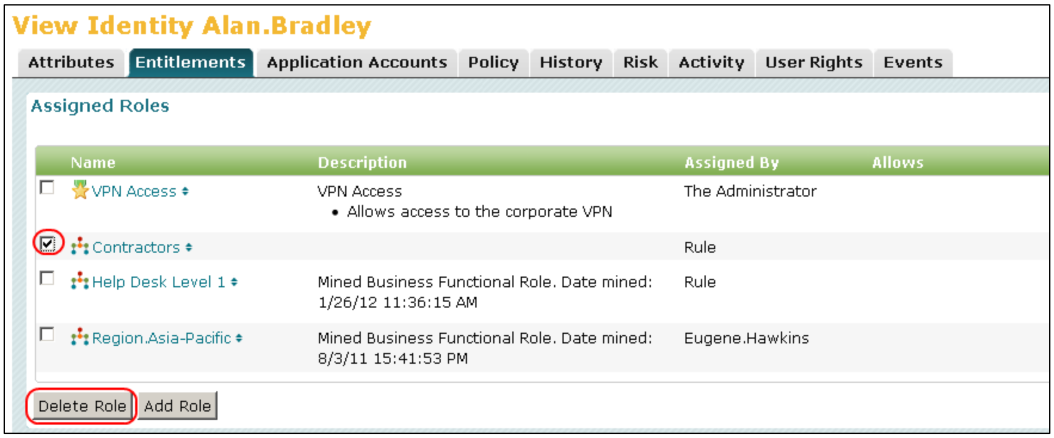
```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Workflow PUBLIC "sailpoint.dtd" "sailpoint.dtd">
<Workflow created="1317235066812" explicitTransitions="true" id="40288f0132ac2fb50132b15407bc0018" libraries="Identity" name="Lif
  <Variable input="true" name="trigger">
    <Description>The IdentityTrigger</Description>
  </Variable>
  <Variable input="true" name="event">
    <Description>The IdentityChangeEvent</Description>
  </Variable>
  <Variable input="true" name="identityName">
    <Description>The name of the identity.</Description>
  </Variable>
  <Variable initializer="script:(identityDisplayName != void) ? identityDisplayName : resolveDisplayName(identityName)" input="true" nam
    <Description>
      The displayName of the identity being updated.
      Query for this using a projection query and fall back to the name.
    </Description>
  </Variable>
  <Variable name="plan">
    <Description>The provisioning plan, which is built by a service method. </Description>
  </Variable>
```

Figure 16: Edit Workflow XML through Debug Pages

Additional Lifecycle Events and Workflows/Business Processes can be created as needed to support each installation's business needs.

Identity Cube Modifications

Users who have access to view and edit information on Identity Cubes (through the **Define** -> **Identities** menu option) can modify the Identity's Assigned Role list directly, either adding or deleting Assigned Roles. Typically only administrators can edit the Identity Cube information in this way. This generates a provisioning request to add or remove the Role and any associated Required Roles (and their Entitlements).



	Name	Description	Assigned By	Allows
☐	VPN Access	VPN Access • Allows access to the corporate VPN	The Administrator	
☑	Contractors		Rule	
☐	Help Desk Level 1	Mined Business Functional Role. Date mined: 1/26/12 11:36:15 AM	Rule	
☐	Region.Asia-Pacific	Mined Business Functional Role. Date mined: 8/3/11 15:41:53 PM	Eugene.Hawkins	

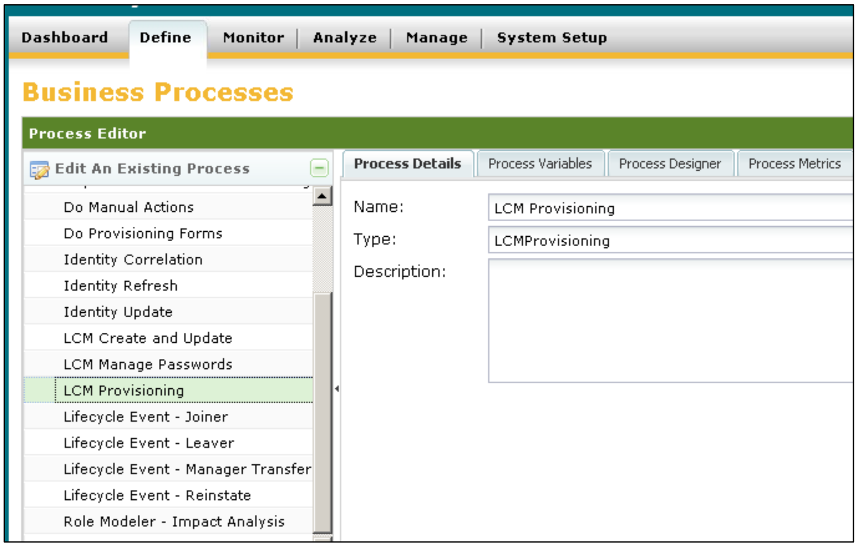
Figure 17: Delete Role on Identity Cube

Note, however, that deleted Roles that were assigned by Rule will be automatically re-assigned to the Identity during the next Identity Refresh unless either the Rule or the Identity's triggering Attributes have changed. The re-assignment is also processed as an Identity-Refresh-driven provisioning request.

Processing Provisioning Requests

When a provisioning request is submitted from any of these sources, IdentityIQ creates a master Provisioning Plan for the requested action(s). In most cases, a Workflow Case is also created to manage and track the provisioning activity's progress. The Workflow Case contains a Workflow that specifies the process to follow.

Pre-defined Workflows, or Business Processes, exist for Identity Change, Identity Refresh, LCM Provisioning, and several Lifecycle Events (Joiner, Leaver, Manager Change, Reinstate). These can be customized for each installation as needed. The Workflow Case created for each provisioning request is associated with the appropriate Workflow for the event that generated the request.



Name: LCM Provisioning

Type: LCMProvisioning

Description:

Figure 18: Defined Workflows (Business Processes)

The Workflows that drive the provisioning process from each request source are shown in the table below.

Provisioning Request Source	Workflow Invoked
Lifecycle Manager (LCM)	LCM Provisioning
Identity Refresh	Identity Refresh
Identity Cube Modifications	Identity Update
Lifecycle Events	Each event is managed by the business process noted in **Business Process** field on the Lifecycle Event definition window
Certification Remediations / Provisioning	None Managed by Perform Maintenance task unless cert specifies "Process Revokes Immediately" (in which case Certification kicks off remediation directly)
Policy Violation Remediations	None; PV Remediations created from Certifications are treated like any other certification remediation PV Remediations created from Manage -> Policy Violations window are managed by Perform Maintenance task

Perform Maintenance Task Involvement

Certification-driven provisioning activities and Policy Violation Remediations do not create a Workflow Case and are not managed through a Workflow. These create Remediation Items that are picked up and processed by the Perform Maintenance task. (The provision-missing-required-roles requests on a certification are not remediation items but are added to the same provisioning plan as "additional actions"; they are managed by the same process as the remediation items.) The Perform Maintenance task invokes the Remediation Manager to process the remediation requests. In the case of Certifications whose specifications include the "Process Revokes Immediately" option, the Certificationer invokes the Remediation Manager directly to process the remediation requests. Regardless, the basic logic of the provisioning process remains the same; the Remediation Manager uses the same mechanisms employed by the workflows to complete the requests.

Overview of Provisioning Process

Provisioning occurs in three phases:

- Plan Compilation: analysis and preparation of the plan for processing
- Template Completion: requesting of missing required data from a user
- Plan Evaluation: submittal of the plan to the appropriate connector to provision the requested access

Plan Compilation

The Plan Compiler is responsible for completing the following tasks:

- Create the Provisioning Project
- Evaluate and expand Roles into individual Entitlement requests
- Apply Provisioning Policies
- Identify Questions for remaining missing information
- Filter and check dependencies
- Partition the full plan into a set of smaller plans: one for each Integration Config, one for each Provisioning Engine connector, and one for all "unmanaged" applications.

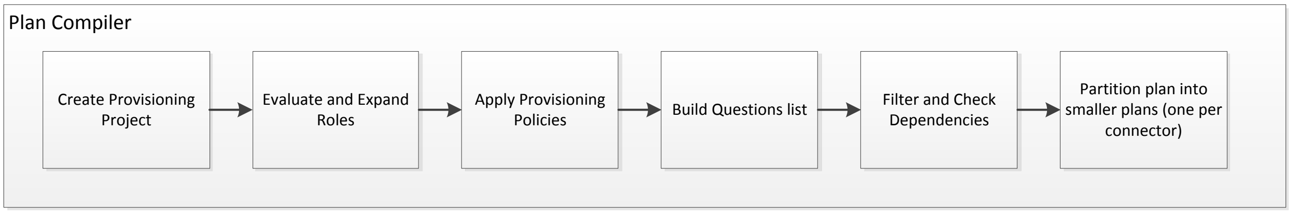

Plan Compiler
Create Provisioning Project
Evaluate and Expand Roles
Apply Provisioning Policies
Build Questions list
Filter and Check Dependencies
Partition plan into smaller plans (one per connector)

Figure 19: Plan Compiler Steps

The Provisioning Project

As Roles are expanded into Entitlement requests, missing information for the requests are identified, and the plan is subdivided into smaller plans, the Provisioning Project will serve as the container for all these pieces. It contains the original (master) Provisioning Plan and encapsulates the entire set of provisioning activities that are part of or required by the original request.

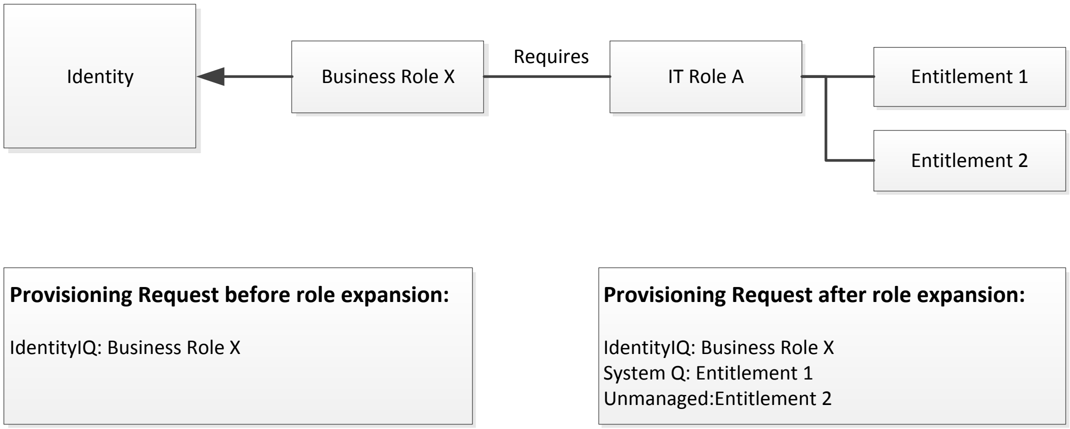
Once the Provisioning Project has been created, master lists of all account requests, attribute requests, and permission requests are created within the project. These are used to catalog all of the individual requests needed to fulfill the plan so they can be partitioned into smaller provisioning plans per application in a later step.

Role Evaluation and Expansion

The master plan is evaluated to determine whether it contains any role assignments. If it does, those roles must be expanded. Role expansion is the process of identifying IT roles required by an assigned Business Role and then determining what specific Entitlements are required by the IT role, adding the Entitlements to the provisioning project's lists of account/attribute/permission requests.

For example, Business Role X is added to an Identity. Business Role X requires IT Role A (which in turn has Entitlements associated with it). The Plan Complier sees that IT Role A is required, identifies its necessary Entitlements, and adds the Entitlements to the project.

NOTE: After role expansion is complete, "IT Role A" will not appear in the project at all; only the raw Entitlements required by IT role A will be listed.



Provisioning Request before role expansion:

IdentityIQ: Business Role X

Provisioning Request after role expansion:

IdentityIQ: Business Role X
System Q: Entitlement 1
Unmanaged:Entitlement 2

Figure 20: Role Expansion

Applying Provisioning Policies

Sometimes provisioning requests require additional information to complete them. This may be because the required information (perhaps for a new account or additional required role) is not provided in the original request. It may be because multiple possible valid values for a field exist with ambiguity as to which is the appropriate choice for the request. This unknown data can often be determined by applying the provisioning policies specified for the Role or the Application involved.

Role Provisioning Policies

Provisioning Policies on Roles serve one primary purpose: to disambiguate the profile. In some cases, the set of Entitlements to be provisioned for an IT Role are easily discerned by looking at the Role Profile. When the role profile terms are all "AND'd" together, IdentityIQ can easily analyze the role profile and provision entitlements that would match the profile. For example, say a role profile has a list of AND'd terms: location='Austin' and memberOf='Engineering'. To satisfy this role, the identity must have both of these account attributes, so requests for those two attributes are added to the plan.

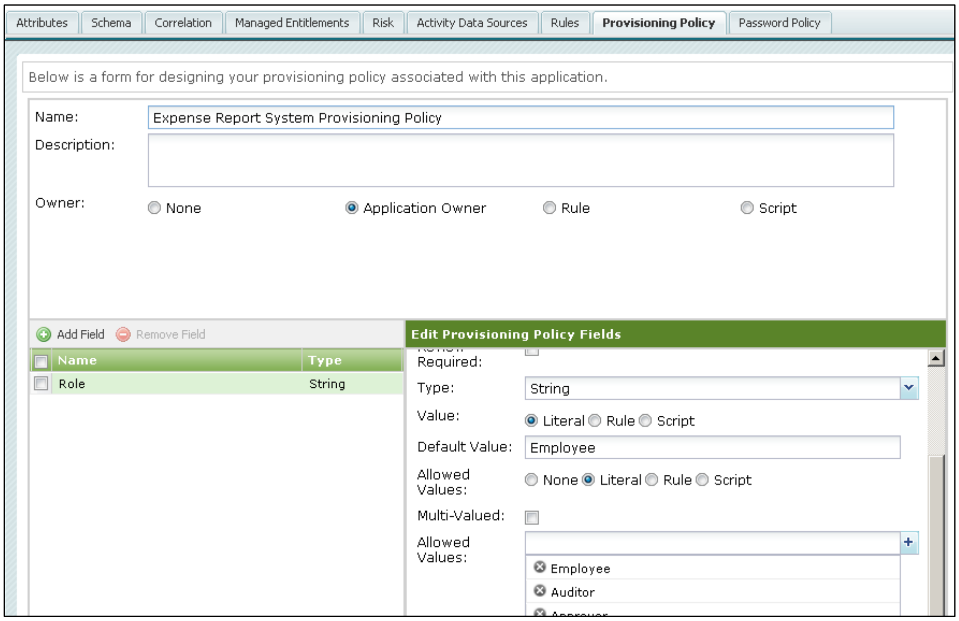
However, a profile that includes a list of OR'd terms: memberOf='Engineering' OR memberOf='Sales’ is ambiguous, since two different memberOf values can satisfy the role. The default provisioning behavior for profiles containing OR terms is to provision only the first one. So in this case, memberOf='Engineering' would be added to the plan but not memberOf='Sales'. For roles with complex profiles the default rules used to convert the profile into provisioning requests may not be enough. Instead, a role provisioning policy must be defined.

A provisioning policy is a list of fields whose names correspond to the name of an Application account attribute used by the role. If the organization would rather have memberOf='Sales" be provisioned for new role members, a provisioning policy could be defined with one field named "memberOf" with the field value "Sales." Fields can also be assigned scripts or rules that allow the appropriate value to be calculated instead of using a hard-coded value.

Application Provisioning Policies

Provisioning Policies can be specified for applications as well. These policies are applied when a new account is requested on that application. Like Role Provisioning Policies, Application Provisioning Policies can specify the field values as literals or through a script or rule.

NOTE: IdentityIQ 5.5 introduced three separate provisioning policies per application: Create, Update, and Delete. With these, different policies can be specified for each of these types of actions on an account for the application -- not just new account creation.



Below is a form for designing your provisioning policy associated with this application.

Name: Expense Report System Provisioning Policy

Description:

Owner: ○ None ● Application Owner ○ Rule ○ Script

□ Name	Type
□ Role	String

Required: □

Type: String

Value: ● Literal ○ Rule ○ Script

Default Value: Employee

Allowed Values: ○ None ● Literal ○ Rule ○ Script

Multi-Valued: □

Allowed Values:

- Employee
- Auditor

Figure 21: Application Provisioning Policy Creation

Identifying Questions

Even after applying the provisioning policies, some pieces of data may still be missing. In fact, some provisioning policies are explicitly written so the data must be obtained from a person at the time the role or application account is requested. These missing data elements are recorded as “questions” on the provisioning project. They will eventually be presented to a person who must provide the information necessary to complete the provision request (during the Template Completion phase).

Dependency Checking and Filtering

During this step of the compilation process, the Identity’s current state is examined and any Entitlements requested in the plan that already exist for the Identity are removed from the plan. Additionally, Entitlements that will be removed based on a Role removal are examined to ensure that they are not also required by another Role held by the Identity; if they are, the Entitlement removal request is taken out of the plan. These actions streamline the provisioning process and prevent unintended consequences of the requests.

Plan Partitioning

At the end of plan compilation, all the individual Entitlement requests identified from the original master plan and the role expansion are partitioned into multiple smaller provisioning plans – one per target. The targets are designated by the connector through which IdentityIQ communicates with them – either a Provisioning Engine read-write connector or an Integration Executor (with its associated Integration Config). Any requests in the plan that cannot be handled by any of the Integration Configs or read-write connectors are added to the “unmanaged plan;” requests in the unmanaged plan will be processed manually through IdentityIQ WorkItems.

Template Completion

When plan compilation is over, the project may still contain some unanswered questions that must be presented to a person to answer. Responsibility for getting these answers falls to the component controlling the provisioning process – namely, the workflow. The provisioning broker itself does not interface with users and therefore has no ability to get these questions answered.

NOTE: The processes that manage Certification remediations / provisioning activities and policy-violation remediations cannot present forms to users, so this phase does not apply for those provisioning activities. These requests will only be fulfilled if they can be completed with the available information. In general, this is only a potential issue with missing-required-role provisioning activities, since remediation requests are access removal requests that should not require any additional data.

Presentation of Provisioning Forms

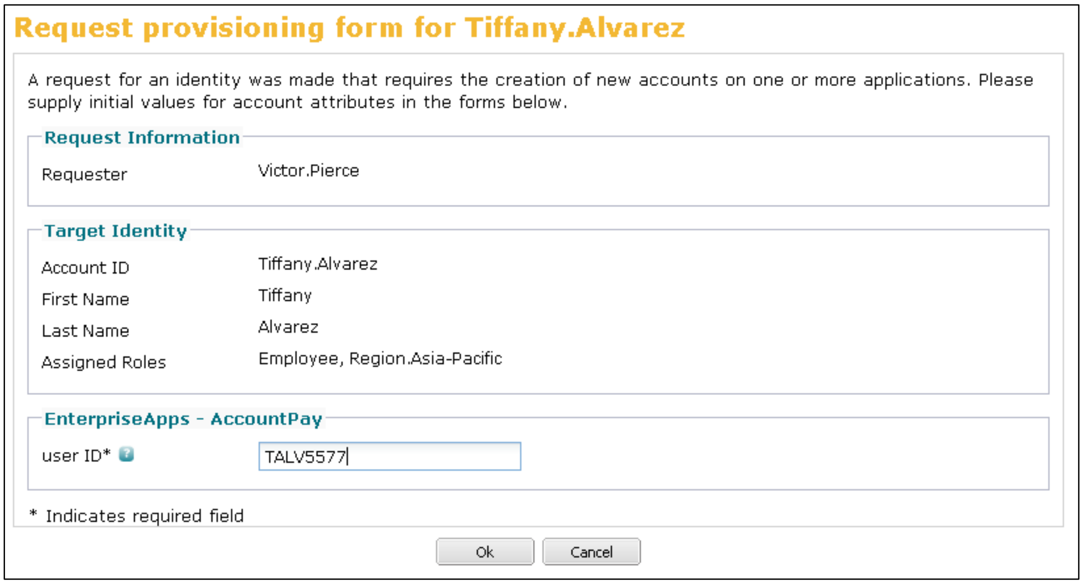
The LCM Provisioning, Identity Refresh, and Identity Update workflows all invoke the Do Provisioning Forms business process to present the questions on user-facing forms and collect the answers. The Do Provisioning Forms process further subdivides these actions into these steps:

- Build Provisioning Form

- Present Provisioning Form
- Assimilate Provisioning Form

Provisioning Policy fields themselves can optionally be assigned an owner; when an owner is assigned, any questions related to the field are sent to that field owner for answers, rather than being presented to the access requester. The controlling workflow is responsible for identifying which questions go to whom and submitting the forms to the right Identities.

The LCM Provisioning Workflow contains by default two different opportunities to present provisioning forms to a user (steps called “Do Provisioning Forms Pre-Approval” and “Do Provisioning Forms Post-Approval”, both of which execute the Do Provisioning Forms workflow). Questions answerable by the original requester are presented before approval so they can be answered at the time the request is submitted. Questions that must be directed to other individuals are presented after approvals are in place to prevent unnecessary work on requests that may be rejected by an approver.



Request provisioning form for Tiffany.Alvarez

A request for an identity was made that requires the creation of new accounts on one or more applications. Please supply initial values for account attributes in the forms below.

Request Information

Requester	Victor.Pierce

Target Identity

Account ID	Tiffany.Alvarez
First Name	Tiffany
Last Name	Alvarez
Assigned Roles	Employee, Region.Asia-Pacific

EnterpriseApps - AccountPay

user ID*	TALV5577

* Indicates required field

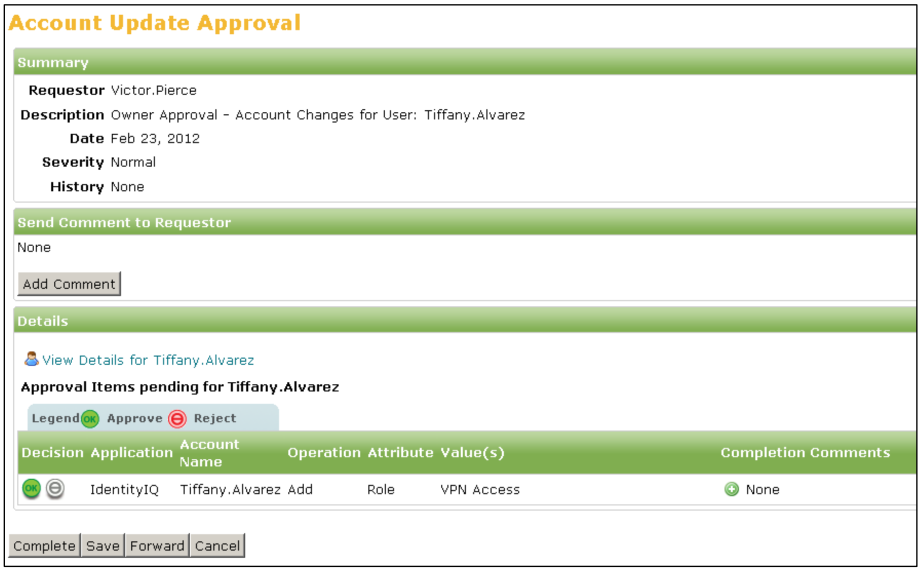
Figure 22: Provisioning Form (based on IT Role Provisioning Policy)

Extra Approval Step for LCM

The LCM Provisioning Workflow contains an approval process during the Template Completion phase that does not occur in other workflows as they exist out of the box. LCM Provisioning requests can be submitted for up to three levels of approval before being executed (always routed in this order to as many of these as are specified in the workflow’s approvalScheme process variable):

- Identity’s Manager
- Object (Role or Application) Owner
- Security Officer (Identity must be specified in process variable securityOfficerName)

If the request is submitted *by* the Identity’s Manager, that approval is considered implicit and is bypassed in the approval workflow.



Account Update Approval

Summary

Requestor Victor.Pierce
Description Owner Approval - Account Changes for User: Tiffany.Alvarez
Date Feb 23, 2012
Severity Normal
History None

Send Comment to Requestor

None

Details

View Details for Tiffany.Alvarez

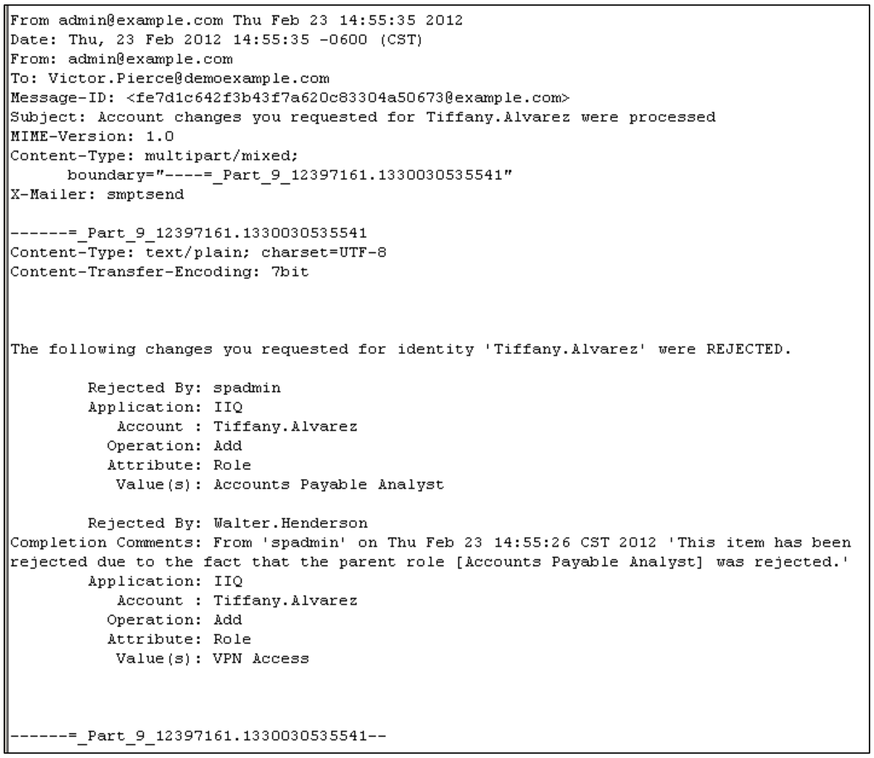
Approval Items pending for Tiffany.Alvarez

Legend ✓ Approve ⊖ Reject

Decision	Application	Account Name	Operation	Attribute	Value(s)	Completion Comments
✓ ⊖	IdentityIQ	Tiffany.Alvarez	Add	Role	VPN Access	None

Figure 23: LCM Provisioning Approval Request (Sent to Role Owner per approvalScheme variable value)

If any approver rejects any part of the request, the rejected action is not executed, and the requester and the Identity for whom the request was made are notified of the rejection. Approved portions of the plan continue through execution. Note, however, that if an assigned role is rejected, its permitted roles will automatically be rejected as well because of their dependence on the assigned role.



```
From admin@example.com Thu Feb 23 14:55:35 2012
Date: Thu, 23 Feb 2012 14:55:35 -0600 (CST)
From: admin@example.com
To: Victor.Pierce@demoexample.com
Message-ID: <fe7d1c642f3b43f7a620c83304a50673@example.com>
Subject: Account changes you requested for Tiffany.Alvarez were processed
MIME-Version: 1.0
Content-Type: multipart/mixed;
      boundary="----=_Part_9_12397161.1330030535541"
X-Mailer: smptsend

------=_Part_9_12397161.1330030535541
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit



The following changes you requested for identity 'Tiffany.Alvarez' were REJECTED.

        Rejected By: spadmin
        Application: IIQ
           Account : Tiffany.Alvarez
          Operation: Add
          Attribute: Role
           Value(s): Accounts Payable Analyst

        Rejected By: Walter.Henderson
Completion Comments: From 'spadmin' on Thu Feb 23 14:55:26 CST 2012 'This item has been
rejected due to the fact that the parent role [Accounts Payable Analyst] was rejected.'
        Application: IIQ
           Account : Tiffany.Alvarez
          Operation: Add
          Attribute: Role
           Value(s): VPN Access


------=_Part_9_12397161.1330030535541--
```

Figure 24: Email Notifying Requester of Request Rejection

Plan Execution

Once the plans have been partitioned and any missing fields have been provided, the subdivided plans can be executed. The Plan Executor passes the partitioned plans to the mechanism responsible for carrying out the request. Results are recorded in the plan to indicate whether the request was carried out immediately (and successfully) or whether it was queued for execution in the future. This status determines when the Identity Cube is updated to reflect the provisioned changes (see Updating the Identity Cube).

Plans are executed through one of these three mechanisms:

- Integration Executors
- Provisioning Engine Read-Write Connectors
- Internal work items

Integration Executors

Some applications connect to IdentityIQ through one-way, read-only connectors, designed only for aggregating data into IdentityIQ from those applications. Writing data back out to those applications is managed separately through an Integration Executor. Parameters for communicating with the applications through the Integration Executors are specified in Integration Configurations (or Integration Configs). Integration Configs are used to manage provisioning to other Provisioning Systems (e.g. SIM, OIM, Tivoli, Novell, BMC ESS), provisioning to Remedy (creating tickets in the help desk system), and custom provisioning using Provisioning Table Integration.

Integration Executors attempt an immediate update of the target application and then queue the activity if the immediate update attempt is unsuccessful. However, regardless of whether the activity commits immediately or not, the Integration Executors are unable to communicate back to IdentityIQ when the request was completed, so these requests are always considered queued.

Provisioning Engine Read-Write Connectors

Read-write connectors are available to manage data communication between IdentityIQ and an ever-increasing number of applications. These connectors are also referred to as the Provisioning Engine Connectors. For applications using these connectors, parameters for managing provisioning activities with the application can be found in its Provisioning Config.

Provisioning with these applications is fully automated. These connectors generally execute the plan immediately and can report back a “committed” status to IdentityIQ in real time, confirming that the changes can be reflected on the Identity Cube immediately.

IdentityIQ Updates

A separate plan is also created for items that require updates to IdentityIQ itself, such as roles assigned to an Identity. Though no connector is required to complete these internal updates, these requests most closely resemble Provisioning Engine Connector updates in that they are executed immediately and are reported back as “committed” at the time of update.

Work Items

After the Integration Executors and Provisioning Engine Connectors have all been called, the unmanaged plan is examined. The unmanaged plan includes provisioning requests to any application from which data is aggregated via read-only connectors but which does not have an Integration Executor that communicates with it. These applications must have their provisioning requests completed through a process that is outside of IdentityIQ’s control or involvement.

The unmanaged plan’s execution is overseen by the controlling workflow or Remediation Manager, rather than by the Plan Executor; in the workflows, this is the “Do Manual Actions” step. If the unmanaged plan contains any requests, one or more Work Items are opened in IdentityIQ that contains the provisioning instructions from the plan. Each Work Item is assigned to an Identity (often the application or entitlement owner) who is responsible for implementing the changes required to complete the specified provisioning tasks. When the provisioning action has been completed, the assigned Identity must manually mark the Work Item as “complete”.

Provisioning tasks managed through work items are considered queued, rather than committed, even if the assigned user marks the Work Item complete. This is because IdentityIQ cannot know with certainty whether the changes were actually made or not until after the next aggregation from the source application.

Plan Initializer Rule or Script

Integration Configs and Provisioning Configs both allow a Plan Initializer Rule or Script to be specified for them that can carry out installation-specific pre-processing during plan execution. If either is specified, it is run immediately prior to carrying out the provisioning activity requested through that config’s application or integration executor.

Updating the Identity Cube

Except in the case of provisioning activities that occur wholly within IdentityIQ itself (such as assigning a business role to an Identity), the provisioning action itself does not actually change the information on the Identity Cube. For example, simply executing a provisioning plan will not update role detections. An Identity Refresh is necessary to update the Identity based on the provisioned items, such as updating the list of detected Entitlements and Roles. Consequently, either the workflow must contain an Identity Refresh step or an Identity Refresh task must be run after the workflow completes.

In general, provisioning workflows includes an Identity Refresh step that can be enabled or disabled as appropriate to the provisioning activity. For Provisioning Engine read-write connectors that process requests immediately, the Identity Refresh step is usually enabled. This is because the changes to application accounts made by those connectors are usually reflected immediately in IdentityIQ. The Refresh can, therefore, immediately update the list of detected Entitlements and roles for the Identities. (Enabling the Refresh step in the "LCM Provisioning" workflow, for example, requires setting the doRefresh variable to True.)

However, requests that were queued will not be applied to the Identity Cube until a re-aggregation has occurred from the application involved, showing that the request was completed. As a result, the Identity Refresh step is commonly disabled for provisioning workflows that are managing Integration Config-driven provisioning activities, since the refresh would not be able to detect any changes until after an aggregation from the source system.

Items that were processed as WorkItems from the unmanaged plan are treated as queued requests, since manually closing a WorkItem does not necessarily mean all the work has been completed. Only a re-aggregation from the source system will confirm that the request was processed. Again, this aggregation must be followed by an Identity Refresh to update the Identity Cube with the information.

NOTE: The Identity Cube's Application Accounts tab reflects account data (as recorded on the Link object for the Identity), so it will show the provisioned access immediately following the read-write connector's "commit" or following a re-aggregation from Integration Config-managed applications. However, the Entitlement data (shown on the Entitlement tab and in any Certification) is not updated until the Identity Refresh task has run.

Special Case: Optimistic Provisioning

There is one case in which IdentityIQ will reflect provisioned changes before they have been confirmed through re-aggregation: when the workflows are configured for Optimistic Provisioning. Optimistic Provisioning assumes that provisioning requests will be completed and updates the Identity Cube to reflect the changes when the request has been submitted, rather than when it has been verified.

To configure the workflows for Optimistic Provisioning, set their "optimisticProvisioning" Process Variable (or XML arg) to True. Most of the provisioning-related workflows are configured with this argument by default; others could be modified to add it and update the Identity Cube based on its being set to true.

In general, this configuration is useful for some testing scenarios or product demonstrations, but it is not an ideal configuration for most production environments. Most companies prefer for IdentityIQ to reflect a confirmed state of system access, rather than a desired state.

Summary of Workflows, Tasks, and Rules in Provisioning

This table provided the reader with an at-a-glance list of workflows, tasks, and rules that may be involved in provisioning through IdentityIQ.

Type	Name	Purpose / Usage
Workflow	LCM Provisioning	Manages provisioning actions requested through LCM
Workflow	Identity Update	Manages the provisioning actions required based on an Identity Cube update
Workflow	Identity Refresh	Manages the provisioning actions required from an Identity Refresh
Workflow	Lifecycle Event – Joiner Lifecycle Event – Manager Change Lifecycle Event – Leaver Lifecycle Event – Reinstate	Controls the Lifecycle Event-driven activities, which may contain provisioning actions
Workflow (subprocess)	Do Provisioning Forms	Creates, presents, and gathers data from provisioning forms (Template Completion phase of provisioning)
Workflow (subprocess)	Do Manual Actions	Presents the unmanaged portion of a provisioning project as work items to be processed manually. This is used by the Identity Update and Identity Refresh workflows. (LCM has a similar step but it audits differently.)
Workflow (subprocess)	Provision with Retries	Manages retries on the provisioning actions for LCM.
Workflow (subprocesses)	Identity Request Initialize Identity Request Violation Review Identity Request Approve Identity Request Approve Identity Changes Identity Request Provision Identity Request Notify Identity Request Finalize	New in release 5.5; these subdivide LCM Provisioning into more manageable workflow pieces (some are also used by Lifecycle Event workflows)
Task	Identity Refresh	Creates provisioning requests based on application of Role assignment rules/Role detection
Task	Perform Maintenance	Processes Certification- and Policy Violation-generated remediation requests
Task	Account Aggregation	Provisioning activities driven by Integration Configs or Work Items require a re-aggregation from the target system before the Identities will be updated to reflect the access change
Rule	FieldValue	Identifies Provisioning Policy Field's default value
Rule	AllowedValues	Constrains Provisioning Policy Field's allowed values
Rule	Validation	Defines validation process for Provisioning Policy Field
Rule	Owner	Defines owner for Provisioning Policy Field
Rule	PlanInitializer	Can be specified for any IntegrationConfig or ProvisioningConfig to run installation-specific pre-processing in Plan Evaluation step before carrying out

		provisioning
Rule	IdentityTrigger	Can determine triggering of a Lifecycle Event

Document Revision History

Revision Date	Written/Edited By	Comments
Feb 23, 2012	Jennifer Mitchell	Initial Creation (current release: 5.5)