Provisioning

Version: 8.4

Revised: September 2023

Copyright and Trademark Notices

Contents

Provisioning with IdentityIQ

The IdentityIQ provisioning capabilities help companies manage system access for their personnel. Provisioning requests can be created and processed in several ways in IdentityIQ, based on the needs and configuration of the installation. In many cases, modifications to access or entitlements you request in IdentityIQ can be automatically reflected in the associated native applications.

This chapter traces the flow of the provisioning plan through its evaluation and preparation for processing into the appropriate native system. Included throughout are the IdentityIQ tasks, business processes and rules that operate on the data as it moves through the process.

> Note: Business processes are often referred to as workflows.

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

- The provisioning request is made through one of several actions or activities.
- The request is created as a provisioning plan.
- The Provisioning Broker evaluates and compiles the provisioning plan, which often involves dividing the original plan into several partitioned plans. Each partitioned plan addresses a single application.
- Each partitioned provisioning plan is passed to the appropriate handler.
    - For integration configuration or read-write connectors, the change is written to the destination system.
    - For Work Items, a work item is created and assigned to an identity who must for manually process the request into the target system.
- The provisioning actions are confirmed and marked on the identity cube, based on the mechanisms involved.

Use the Administrator Console link, under the gear icon, to access the Provisioning Transactions table to view the status of all provisioning transactions in your implementation of IdentityIQ; connectors, manual work items, and IdentityIQ operations. Refer to the **System Administration** documentation.

Access to the Provisioning Transaction table is controlled with IdentityIQ rights.

Recording Provisioning Requests

You can create provisioning requests in IdentityIQ using any of the following actions or activities:

- Certifications
- Policy Violations
- Identity-Refresh-Driven Assignments
- Lifecycle Manager Requests
- Lifecycle Event-Driven Provisioning

Provisioning requests create a provisioning plan that the Provision Broker can analyze and process. In all cases, except certification and policy violation-generated requests, provisioning requests create a Workflow case. The Workflow case manages the processing of the provisioning request based on a defined Workflow. See also Processing Provisioning Requests.

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. This certification process can result in:

- **Certificate Remediation** – When an identity's access to a system is determined to be inappropriate for their job function, the certifier can revoke the entitlement through the Certification Access Review. This process creates a remediation provisioning request in IdentityIQ to remove that access from the source application.
- **Provisioning through Certifications** – When a business role is approved for an identity and that role includes required IT roles the identity does not have, the certifier is prompted to select whether the missing roles must be provisioned for the identity or whether the business role must be approved without provisioning the missing roles. If the certifier elects to provision the missing roles, a provisioning request is created.

> 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.
>
> All revocations and provisioning requests from a specific access review are combined into a single provisioning plan and processed together except in certifications where revocations are processed immediately, such as certifications with the Process Revokes Immediately setting selected.

Policy Violations

Policies defined in IdentityIQ enable the system to evaluate an identity's access or activities and report any inconsistencies with company policies. Violations are reported to the violation owner, often the identity's manager, or the appropriate application owner. The violation owner can then permit an exception or initiate a remediation request. The following types of policy violation remediations are available:

- Policy Violation Remediations for SOD Policy Violations
- Policy Violation Remediations for Non-SOD Policy Violations

Policy Violation Remediations for SOD Policy Violations

Only remediations for role or entitlement Separation of Duties (SOD) violations generate a provisioning request to revoke the invalid access. For example, when a manager evaluates an identity's SOD violations and determines that one of the accesses for the identity must be removed, the manager can request the revocation of the invalid access.

You can create policy violation remediation requests from:

- Policy owner's Policy Violation page that you can from **Manage -> Policy Violations** page.
- Certification on which the violation is noted.

Policy Violation Remediations for Non-SOD Policy Violations

> Note: By default, you cannot remediate non-SOD policy violations with a certification or in the policy violation window.

You can perform the following actions to enable certification remediate and generate a Work Item:

1. Edit the XML for any policy to include **remediated** as one of its certificationActions values to enable certification remediation on that policy type.
2. Select the remediation option for the violation in a certification to automatically create a Work Item that informs the appropriate party of the need to manually correct the violation.

Identity-Refresh-Driven Assignments

You can use the following options on an Identity Refresh task to generate provisioning requests for identities:

- **Refresh assigned, detected roles and promote additional entitlements** — Creates provisioning requests for IdentityIQ to add roles to identity cubes.

- **Provision assignments** — Creates provisioning requests that apply to external applications.

The following table describes these options in more detail:

Option	Description
Refresh assigned, detected roles and promote additional entitlements	Runs the defined assignment rules for roles and examines role detection profiles to update the Assigned and Detected role lists for the identity. This option does NOT provision access in external system
	Generates provisioning requests to add entitlements required by the currently assigned roles, which can include: - Entitlements for newly assigned roles - Entitlements missing from previously assigned roles. If a role was previously assigned through an automatic assignment rule and the rule no longer returns true, provisioning requests are generated to remove the entitlements that the role requires. If another assigned role requires those entitlements, they are not removed.

> Note: By default, the entitlements associated with a role are de-provisioned 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 is a separately licensed portion of the IdentityIQ product that is designed to manage entitlements using provisioning requests. Based on their manager status and how the Lifecycle Manager is configured, users can make requests for themselves or for other identities.

In a typical configuration:

- Managers can make requests for their direct reports.
- Help desk users can make requests for themselves and others.
- Any user can make requests for themselves.

Lifecycle Manager Toolbar

When Lifecycle Manager is enabled, the Lifecycle Manager toolbar displays at the top of the IdentityIQ view and supports the following actions:

- Request Access
- Manage Accounts
- Other Lifecycle Manager Options

> Note: The set of identities for which these actions can be taken is based on the individual user's authority and the Lifecycle Manager configuration. The self-service, Request For Me, options do not include Create Identity.

Request Access

Request Access includes Role and Entitlement requests. If you are working with a single user, a third tab, **Current Access** displays that you can use to request the removal of Roles or Entitlements. Use the Lifecycle Manager Request Roles feature to generate requests that:

- Add the appropriate role to the specified identities.
- Provision the entitlements the role requires.
- Provision permitted roles, if added to the request when prompted.
- Deprovision by removing roles from an identity
  This option generates a provisioning request to remove the role assignment from the identities and the entitlements the role requires if another role does not need the entitlements.

Use the Lifecycle Manager **Request Entitlements** feature to generate requests to:

- Add the entitlement to the specified identity.
- Revoke an identity's current entitlements.
  This option generates a provisioning request that removes the access from the source application or applications.

By default, when you request a new entitlement on an application and the user already has an account on that application, the entitlement is added to the existing account. If needed, you can create a separate account for specific entitlements.

To create multiple accounts for a single identity on an application or to add an entitlement to a specific existing account when several are available:

1. Navigate to the Lifecycle Manager configuration Additional Options page.
2. In the **General Options** section, select an application included in the list for **Applications that support additional account requests**.
3. For the **Account** selection, select the option to create a new account or the option to add the entitlement to an existing account that the identity already has.

Manage Accounts

Use the **Manage Accounts** feature to:

- Request accounts on additional applications – generates provisioning requests.
- Revoke or disable existing accounts – generates provisioning requests.
- Enable disabled accounts – generates provisioning requests to enable or disable accounts.
- Unlock locked accounts – generates provisioning request.

To use the Manage Accounts to request a new account:

1. Navigate to the Lifecycle Manager configuration Additional Options page.
2. In the **Manage Accounts Options** section, select an application included in the list of applications that support account-only requests.
3. For the **Account** selection, select the option to create a new account or the option to add the entitlement to an existing account held by the identity.

> Note: You can also select the Manage Accounts option on the Lifecycle Options page for any group, they can enable, disable, and delete accounts for the existing accounts. The connector must support this action and the action must not be disabled through another setting on the Additional Options page.

Other Lifecycle Manager Options

Other Lifecycle Manager options include the following items:

- **Create Identity** – Creates provisioning plans that update IdentityIQ. You can create a new IdentityIQ identity with a set of attributes that can be configured. The attributes that you can set or change are defined by a form that can be customized. New identities do not have accounts on any application.

- **Edit Identity** – Creates provisioning plans that update IdentityIQ. You can modify attributes for an existing IdentityIQ identity. The attributes that you can set or change are defined by a form that can be customized.

  > Note: Life Cycle Events can cause provisioning outside of IdentityIQ or additional provisioning inside IdentityIQ. In addition. Attribute sync can also cause provisioning outside of IdentityIQ based on create or edit identity.

- **Manage Passwords** – Resets passwords on target systems which involves a provisioning plan and provisioning action.
- **View Identities** – Does not have provisioning-related functionality and is read-only.

Lifecycle Event-Driven Provisioning

With Lifecycle Manager enabled, Lifecycle Events can be configured in IdentityIQ to represent activities that occur during the normal course of a person's employment at a company. These activities include events such as joining the company, changing departments or managers, and leaving the company. The shorthand terms for these activities are Joiner, Mover and Leaver.

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

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

By default, these events are disabled and must be enabled before the events can be triggered. Lifecycle Events are triggered by specific changes to an identity. These changes can include the following actions:

- Creation
- Manager transfer
- Attribute change
- Complex changes that an IdentityTrigger rule detects

The triggered Lifecycle Events invoke business processes, or workflows, that can contain provisioning actions.

> Note: The terms Business Process and Workflow are synonymous. The IdentityIQ user interface refers to these terms as Business Processes which is the term business managers use most often. The IdentityIQ object model and XML use the term Workflows.

Manage Lifecycle Events and Actions

The Lifecycle Events and the default actions of each of the business process that the pre-defined Lifecycle Events invoke are listed below.

- **Lifecycle Event – Joiner** — Prints the name of the identity to sysout. No actions are taken on the identity. This action is typically modified to provision birthright access for identities.
- **Lifecycle Event – Leaver** — Creates and runs a provisioning plan to disable all accounts the leaving identity has.
- **Lifecycle Event – Manager Transfer** — Prints names of the old and new manager to sysout. No actions are taken on identity or entitlements. This action is typically modified to generate a certification for the new manager to review the access an identity holds. This action can also be used to provision birthright access identified for members of new manager's group.
- **Lifecycle Event – Reinstate** — Creates and runs a provisioning plan to enable all previously disabled accounts that a returning identity had.

Lifecycle Events and Actions How-To Tasks

You can perform the following tasks for Lifecycle events and actions:

> Note: Additional Lifecycle Events and workflows/business processes can be created as needed to support the business needs for each installation.

How To Edit Pre-defined Lifecycle Events

1. Navigate to **Setup -> Lifecycle Events** page.
2. Right-click an entry and click **Edit** or double click an entry.
3. Make desired changes and click **Save**.

How To Create a New a Lifecycle Event

1. Navigate to **Setup > Lifecycle Events** page.
2. Click **Add New Lifecycle Event**.
3. Enter information for **Lifecycle Event Options** and **Behavior**.
4. Click **Save**.

How To Delete a Lifecycle Event

1. Navigate to **Setup > Lifecycle Events** page.
2. Right-click an entry and select **Delete**.

How To Modify Actions for Lifecycle Events

1. Navigate to Navigate to **Setup -> Business Process** page.
2. Select the **Process Designer** tab.
3. Select a process from the **Edit An Existing Process** list.

> Note: Typically only administrators can edit the Identity Cube information. This option is available through **Identities > Identities Warehouse**.

You can also access IdentityIQ Debug pages and modify actions through the XML Workflow.

See Business Processes documentation for more details.

Other Identity Cube Modifications

In addition to the Lifecycle Manager pages, users with the right capabilities can access an administrative interface to make additional identity modifications. Navigate to the **Identities > Identities Warehouse** page.

Most of the information is read-only, but a provisioning plan is generated that updates an identity when you:

- Edit attribute values on the **Attributes** tab.
- Delete or Move account links from the **Application Accounts** tab.
- Change capabilities or assigned scopes on the **User Rights** tab.

If the triggering attributes for the identity have not changed, deleted roles that were assigned by rules are automatically re-assigned to the identity during the next identity refresh. The re-assignment is also processed as an identity-refresh-driven provisioning request.

Processing Provisioning Requests

IdentityIQ creates a master provisioning plan for the requested actions when a provisioning request is submitted from a provisioning request source. A workflow case is also created to manage and track the progress of the provisioning activity. The workflow case contains the workflow that specifies the process to follow.

> Note: Certification and policy violation based provisioning does not use workflows.

IdentityIQ ships with pre-defined workflows or business processes which 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. The following table lists the Workflows that drive the provisioning process from each request source.

Provisioning Request Source	Workflow Invoked
Lifecycle Manager	Main workflows include: LCM Create and Update, LCM Manage Password, LCM Registration and LCM Provisioning
Identity Refresh	Identity Refresh
Define Identities	Identity Update
Lifecycle Events	Each event is managed by the business process listed in **Business Process** field on the Lifecycle Event definition window.
Certification Remediations / Provisioning	None Managed by and RemediationManager class. If the certification specifies **Process Revokes Immediately**, certification starts the remediation process directly.
Policy Violation Remediations	None Policy violations remediations that certifications create are managed the same as any other certification remediation. Policy violations remediated from **Policy Violations** page are saved directly to the violation table.

Involvement

The **Perform Maintenance** task processes all certification remediation including: roles entitlements and policy violations. This task invokes the Remediation Manager to process the remediation requests.

For certifications with specifications that include the **Process Revokes Immediately** option, the Certificationer object invokes the Remediation Manager directly to process the remediation requests. The basic logic of the provisioning process remains the same. The Remediation Manager uses the same mechanisms that the workflows use to complete the requests.

Remediation tasks that are performed on the **Policy Violations** page are not a part of these maintenance task processes.

> Note: Requests on a certification for provision-missing-required-roles are not remediation items. These requests are added to the same provisioning plan as additional actions. The process that manages remediation items also manages these requests.

Overview of Provisioning Process

The Provisioning Process has three phases:

- Compiling the Plan – Analysis and preparation of the plan for processing
- Answering Provisioning Policy Questions – Request of missing required data from a user
- Implementing the Plan – Submittal of the plan to the appropriate connector to provision the requested access

Compiling the Plan

The Plan Compiler is responsible for the following tasks:

Create the Provisioning Project

The Plan Compiler calculates plans for provisioning using IntegrationConfig objects. Some details of application objects are maintained as an in-memory cache and, because of the cached nature of the objects, an update to an Application or an IntegrationConfig might not immediately take effect for plan calculations.

By default, cache updates are performed every 10 minutes. To modify this, in a test or deployment environment, modify the following SystemConfiguration options:

Evaluate and Expand Roles

The master plan is evaluated for any role assignments. If the plan contains role assignments, those roles must be expanded. The role expansion process:

- Identifies IT roles that an assigned business role needs.
- Determines what specific entitlements the IT role needs.

- Adds the entitlements to the lists of account/attribute/permission request for the provisioning project. Each attribute is represented as an Attribute Request or a Permission Request.

For example, Business Role X is added to an identity. Business Role X requires IT Role A which has entitlements associated with its role. The Plan Complier determines that IT Role A is required, identifies the necessary entitlements, and adds the entitlements to the project.

> Note: After role expansion is complete, IT Role A does not display in the project. Only the raw entitlements that the IT role A needs are listed.

Apply Provisioning Policies

A provisioning policy is a list of fields with names that correspond to an application account attribute name the role uses. Provisioning Policies can be used to help complete an access request that has unknown data required for provisioning. When a provisioning request requires additional information to complete the access request, you can apply a provisioning policy specified for the application involved. Examples of additional or unknown data that is required for provisioning include the following items:

Types of Provisioning Policies include:

- Role Provisioning Policies — Removes role uncertainty.
- Application Provisioning Policies — Applied when a new account is requested.

Role Provisioning Policies

The primary purpose of provisioning policies on roles is to remove any uncertainty for the role. In some cases, examining the role profile can determine the set of entitlements to be provisioned for an IT role. Role profiles can be clear or unclear. When all the role profile terms are joined using AND statements, the profile is clear. IdentityIQ can easily analyze the role profile and provision entitlements that match the profile.

For example, A profile that includes a list of OR terms is unclear, because two or more different memberOf values can satisfy the role. The following table provides examples.

Role Profile Example Terms	Type of Terms	Explanation
location='Austin' and memberOf='Engineering'	Profile with a list of AND terms	To satisfy this role, the identity must have both of these account attributes. Requests for those two attributes are added to the plan.

Role Profile Example Terms	Type of Terms	Explanation
memberOf='Engineering' OR memberOf='Sales’	Profile with a list of OR terms	The default provisioning behavior for profiles containing OR terms is to provision only the first one. In this case, memberOf='Engineering' is added to the plan but not memberOf='Sales'. If the organization wants memberOf='Sales’ provisioned for new role members, a provisioning policy can be defined with one field named memberOf with the field value Sales.

> Note: Fields can also be assigned scripts or rules that enable the appropriate value to be calculated instead of using a hard-coded value.

Application Provisioning Policies

Provisioning Policies can also be specified for applications. These policies are applied when a new account is requested on an application. Application Provisioning Policies are similar to Role Provision Policies and can specify the field values as literal values or through a script or rule. The following actions trigger application provisioning policies:

Application Dependency

You can specify an application dependency at the field level when you create a policy. Application dependency works with synchronous connectors and does not work with connectors that queue plans. Application dependencies are enforced during Create operations. For update and delete, the dependencies are ignored.

> Note: IdentityIQ does not undo dependencies during de-provisioning.

To specify an application dependency:

1. Navigate to **Applications -> Application Definition**. On the Provisioning Policies tab of the Application Configuration page select the dependent application for the provisioning.
2. Double-click or right-click the application in the **Application List**.
3. On the Application Configuration page, select the **Provisioning Policies** tab.
4. Define the application dependency at the field level in the **Create Account** and **Create Group** policies.

Application dependency works similar to roles and entitlements. If a dependency is missing, IdentityIQ expands it and executes a Create request for the dependency. If the user has an existing link on a dependent application, IdentityIQ uses the existing link information to derive the value. When there are multiple accounts on the link, the applicable accounts are selected automatically using rules or through an interactive user interface. Selecting an account can be an option to create a new account.

The available attributes are derived from the account schema of all dependent applications. During plan compilation, IdentityIQ reads these properties and determines any new accounts that are required to satisfy the dependency.

During Plan Evaluation, IdentityIQ uses the dependency settings to determine the order that must be used to implement the plan. If a dependency plan fails, all of the dependent plans also fail. If a dependency plan requires a retry, after the retry is successfully completed, the dependent plans are executed. There is special new logic in the Provision with Retries method that loops back to the provisioning step when there are still plans to complete.

There are not transformations (rules) on dependent fields. The evaluation process copies the exact values from the dependency plan or link to the dependent plan.

Identify Questions

After the provisioning policies are applied, pieces of data can still be missing. Some provisioning policies are specifically written so the data must be obtained from a person when the role or application account is requested. These missing data elements are recorded as questions on the provisioning project. These questions are presented to a person who must provide the information necessary to complete the provision request. See Answering Provisioning Policy Questions.

Filter and Check Dependencies

Filter and Check Dependencies streamline the provisioning process and prevent unintended consequences of the requests. During this step of the compilation process:

- The current state of the identity is examined.
- Any entitlements requested in the plan that already exist for the identity are removed from the plan.
- Entitlements that are to be removed, based on a role removal, are examined. This step determines if the identity has another role that requires the entitlement that is scheduled to be removed.

> Note: If the identity has another role that requires that entitlement, the entitlement removal request is taken out of the plan.

Partition the Plan

At the end of plan compilation, all the individual entitlement requests identified from the original master plan and the role expansion are partitioned into a set of smaller provisioning plans – one per target. The targets are designated by

the connector or **integrationConfig** that IdentityIQ uses to communicate with them. Connections can include:

> Note: Any requests in the plan that cannot be processed by any of the integration configurations or read-write connectors are added to the unmanaged plan and are processed manually through IdentityIQ Work Items.

See also Implementing the Plan.

Answering Provisioning Policy Questions

After the plan is compiled, the project can have unanswered questions that must be presented to a person to answer. The provisioning broker does not interface with the user and cannot get answers to these questions. The workflow process, the component that controls the provisioning process, is responsible for getting the questions answered.

Exceptions

Because the following processes can not present forms to users, this interactive provisioning policy phase does not apply for the associated provisioning activities. These requests are only fulfilled if they can be completed with the available information. Because remediation requests are access removal requests, these requests should not require any additional data.

- Processes that manage certification remediations
- Processes that manager provisioning activities
- Policy-violation remediations

Generally projects that have unanswered questions are only an issues if the projects have activities that require a new account to be created for a new assignment or a missing role.

Provisioning Forms

The Lifecycle Manager Provisioning, Identity Refresh, and Identity Update Workflows invoke the Do Provisioning Forms business process. This process presents questions on user-facing forms and collects the answers. The Do Provisioning Forms process separates these actions into the following steps:

- Build Provisioning Form
- Present Provisioning Form
- Assimilate Provisioning Form

Optionally, you can assign owners for individual provisioning policy fields. When an owner is assigned, any questions related to the field are sent to the field owner and not to the access requester. The controlling workflow identifies who receives the questions and then submits the forms to the correct identities.

By default, the Lifecycle Manager Provisioning Workflow contains two opportunities to present provisioning forms to a user, pre-approval and post-approval. The following named steps run the **Do Provisioning Forms** workflow:

- Identity Request Initialize
- Identity Request Provision

A Workflow can have a different number of approval steps between the steps that present provisioning forms. Each approval can modify items in the master plan that cause the project to be recompiled. For example, if an approver rejects one of the role assignments, provisioning questions for an account that role requires might not be needed.

Implementing the Plan

After the plans are partitioned and any missing fields are provided, the subdivided plans can be implemented through one of the following mechanisms:

- Integrations
- Direct Read-Write Connectors
- Work Items

The results are recorded in the plan and indicate if the request was implemented immediately or placed in a queue for future implementation. This status determines when the identity cube is updated to reflect the provisioned changes. See also Updating the Identity Cube.

The following table provides an overview of the provisioning mechanism.

Provisioning Mechanism	Plan Implementation
Integration Executors	Managed plan implementation using integration executors.Starts as an asynchronous process that might not complete immediately.
Direct Read-Write Connectors	Application objects contain the provisioning configuration.
Work Items	Unmanaged plan implementation using the controlling workflow.

Integrations

Integrations are a separately licensed components that communicate with systems within your network. The following table provides and overview of the integration modules and connectors.

System	Module	Connector
Provisioning systems, such as: OIM, ISIM, FIM	Provisioning Integration Modules (PIMs)	Read/write connectors and IntegrationConfigs/Executors
IT Service Management, such as: Remedy, Service Now, HP Service Manager	Service Integration Modules (SIMs)	IntegrationConfigs/Executors
Mobile device management systems, such as: AirWatch, MobileIron, Good Technology	Mobile Integration Modules (MIMs)	Read/write Connectors
IT Security: HP ArcSight	IT Security Integration Module	IntegrationConfigs/Executors
Enterprise Applications: Oracle EBS, SAP Portal, PeopleSoft, Siebel and NetSuite	Enterprise Resource Planning Integration Modules (ERP Integration Modules)	Read/Write Connectors
Mainframe: RACF, CA-Top Secret, CA-ACF2, RACF LDAP and Top Secret LDAP	Mainframe Integration Modules	Read/Write Connectors
Healthcare: Epic and Cerner	Healthcare Integration Modules	Read/Write Connectors
Identity Intelligence/Analytics: SAP GRC	GRC Integration Module	IntegrationConfigs/Executors

Integration Executors attempt an immediate update of the target application. If the immediate update attempt is unsuccessful, Integration Executors, place the activity in a queue.

> Note: Even if the activity does not immediately commit, the Integration Executors cannot communicate back to IdentityIQ when the request is completed. Therefore, these requests are always considered to be queued.

See also Plan Initializer Rule.

Direct Read-Write Connectors

Read-write connectors are available to manage data communication between IdentityIQ and an ever-increasing number of applications. For applications using these connectors, you manage provisioning activities through the variables in the Provisioning configuration for that application.

Provisioning using direct read-write connector with these applications is fully automated. These connectors generally:

- Run the plan immediately.
- Can report back a committed status to IdentityIQ in real time.
- Confirm that the changes can be reflected on the identity cube immediately.

See also Plan Initializer Rule.

IdentityIQ Updates

For items that require updates to IdentityIQ, such as roles assigned to an identity or identity attribute changes, a separate plan is created. These requests are similar to direct connector updates. Although no connector is required to complete these internal updates, the requests are run immediately and are reported back as committed when updated.

Work Items

Work Items, opened in IdentityIQ that contain provisioning instructions, to provision unmanaged plans. The controlling workflow or Remediation Manager is responsible for implementing an unmanaged plan. An unmanaged plan:

- Includes provisioning requests to any application where data is aggregated using read-only connectors.
- Does not have an Integration Executor that communicates with the plan.
- Are identified and examined after the Integration Executors and direct read-write connectors are called.

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 a user who is responsible for implementing the changes required to complete the specified provisioning tasks. Work item assignees are often the application or entitlement owner. When the provisioning action is completed, the work item assignee must manually mark the work item as complete.

> Note: Provisioning tasks managed through work items are considered queued, rather than committed. Even if the assigned user marks the work item complete, IdentityIQ cannot determine with certainty if the changes were actually made until the next aggregation from the source application is completed.

Plan Initializer Rule

You can specify a Plan Initializer rule to run during the implementation of the provisioning plan. An installation-specific rule can be added to integration and provisioning configurations. When a rule is specified, it runs immediately prior to running the provisioning activity for the application. Provisioning is based on the provisioning plan and application associated configuration or integration executor.

See also Implementing the Plan.

Updating the Identity Cube

Provisioning activities that occur completely within IdentityIQ, such as assigning a business role to an identity, are the only provisioning actions that change the information on the identity cube. For example, implementing a provisioning plan does not update role detections. You must perform an Identity Refresh to update the identity based on the provisioned items. For example, to update the list of detected entitlements and roles, you must perform an Identity Refresh.

Identity Refresh

Provisioning workflows generally includes an Identity Refresh step than can be enabled or disabled as needed for the provision activity. To perform an identity refresh to update the Identity Cube, you must:

- Include an Identity Refresh step in the Workflow, or
- Run an Identity Refresh task after the Workflow completes.

To enable the Refresh step in the workflow the doRefresh variable must be set to True.

General Guidelines

Direct Read-write connectors — For Direct read-write connectors that process requests immediately, the Identity Refresh step is generally enabled. The changes to application accounts that the connectors make are usually displayed immediately in IdentityIQ.

Queued Requests — Requests that were queued are not applied to the identity cube until a re-aggregation has occurred from the application involved. As a result, the Identity Refresh step is typically disabled for provisioning workflows that are managing integration configuration-driven provisioning activities, because the refresh can not detect any changes until after an aggregation from the source system.

Items that were processed as Work Items from the unmanaged plan are treated as queued requests, because manually closing a Work Item does not necessarily indicate all the work was completed. To confirm that the request was processed, you must perform a re-aggregation from the source system. This aggregation must be followed by an identity refresh to update the identity cube with the information.

Because the **Application Accounts** tab for the Identity Cube displays account data that is recorded on the Link object for the identity, the tab lists the provisioned access immediately following the read-write connector commit or following a re-aggregation from integration configuration-managed applications. However, the entitlement data on the **Entitlement** tab and in any certification is not updated until the Identity Refresh task has run.

Special Case: Optimistic Provisioning

When the workflows are configured for Optimistic Provisioning, provisioned changes appear in IdentityIQ before the changes are confirmed through re-aggregation. Optimistic Provisioning assumes that provisioning requests are completed and then updates the identity cube to display the changes when the request is submitted, not when the request is verified.

Optimistic provisioning configuration is useful for some testing scenarios or product demonstrations, but it is not an ideal configuration for most production environments. Companies often prefer that IdentityIQ indicates a confirmed state of system access and not a desired state.

To configure the workflows for Optimistic Provisioning:

1. Verify that the workflow has the Set the optimisticProvisioning process variable. By default, most provisioning-related workflows are configured with this argument
2. Set the optimisticProvisioning process variable, or XML arg, option to True. The default value is false.

> Note: To modify other workflows, add the variable and then follow the steps listed above.

Attribute Synchronization

Attribute synchronization is an automated process of synchronizing changes to an Identity Cube's identity attributes (such as name, email, or department) from an authoritative source to target systems.

A simple example is when an employee's name changes – Pat Smith becomes Pat Jones. In this example, Human Resources will change the employee's name, and perhaps the email address, in an authoritative source, such as Active Directory. The changes then need to be propagated out to other accounts that the user has, such as JIRA, Sales Force, Outlook, etc.

Lifecycle events can also trigger attribute changes that need to be synchronized: users joining or leaving the organization, or changes to things like a user's status, job title, manager, or department can all cause changes to user attributes that need to be synchronized to various systems.

Choosing Which Attributes to Synchronize

To configure attribute synchronization, you first choose which attributes should be synchronized, and edit them to set up synchronization targets and behavior.

1. Click **gear > Global Settings > Identity Mappings**.
2. Double-click the attribute you want to edit.
3. The **Target Mappings** section is where you identify the target systems that should be updated with new values for the attribute. You must add targets one at a time, for each target system. To add a new target, click **Add Target.**
4. Enter your **Target** values:
    - **Application**: the target system to be updated when this value changes.
    - **Attribute**: the attribute on the target system that stores this value. The values in the drop-down menu are determined by the application schema defined for this application. See the **Application Configuration documentation** for more information on application schemas.
    - **Transformation Rule**: if the application attribute is represented differently in the target system than it is in the authoritative source (for example, if your target system records full-time versus part-time employment status as a numeric code 1 or 2, but you record that as "Full" and "Part" in IdentityIQ) you can use a BeanShell rule to modify the attribute as it is pushed out to the target.

- **Provision All Accounts**: If the user has more than one account on the target application, check this option to automatically synchronize the value to all accounts. If you leave this option unchecked, the system will prompt someone to choose which accounts to synchronize to, in cases of multiple accounts.

  Click **Add** to save your changes and close the dialog.

5. *Optional*: if you want to use a business process to manage attribute synchronization for this attribute, check the **Sync with Workflow** option in the **Advanced Options** section. See Using Business Processes to Manage Attribute Synchronization for more information on using business processes for attribute synchronization, and on how to set this option globally rather than at the individual-attribute level.
6. Repeat these steps for each additional Target you want to add for this attribute.

How Attribute Synchronization is Triggered

There are two ways attribute synchronization can be triggered in IdentityIQ:

- **Direct Edit to an Identity**: Editing the identity directly in the UI, in the Identity Warehouse's Identity Details Page, or the Edit Identity quicklink. These changes cause the system to immediately process the synchronization. Note that there may be an approval step required for the change, before the synchronization will occur. See the **Identity Management** documentation for more information.
- **Aggregation**: When an attribute change comes through aggregation, attribute synchronization is initiated through a refresh task that has the **Synchronize Attributes** option selected. See the **Tasks** documentation for more details..

Related:

Using Business Processes to Manage Attribute Synchronization

Auditing Attribute Synchronization

Using Business Processes to Manage Attribute Synchronization

You can integrate a business process with attribute synchronization, to let you manage the synchronization of multiple attributes together, in a single request and approval process. If you have Lifecycle Manager implemented, you can use an out-of-the-box business process for managing attribute synchronization. You can also create your own custom business process if you have not implemented Lifecycle Manager, or if you prefer to use custom logic.

You can set a global option so that all attribute synchronization is handled by a business process, or you can choose individual attributes to manage using a business process.

Configuring Attribute Synchronization to Use a Business Process.

To enable a **global** business process for attribute synchronization:

1. Click **gear > Global Settings > IdentityIQ Configuration.**
2. Click the **Identities** tab.
3. In the **Business Processes** section, choose the business process to use for **Attribute Sync**. IdentityIQ provides a standard Attribute Sync business process that meets most use cases; you can edit this business process to tailor it to your needs, and you can also create and choose a custom business process if you prefer.
4. Check the **Always Sync using workflow** option in the **Identity Attributes** section. Leaving this option unchecked means that you can set the option to use the business process individually on each attribute in Identity Mappings.

To enable a business process handling for attribute synchronization **individually** for specific attributes:

1. Follow the steps above to select a business process in the **IdentityIQ Configuration**, but do *not* check the **Always Sync using workflow** option.
2. In the **gear > Global Settings > Identity Mappings** page, click the attribute you want to manage with a business process.
3. In the **Advanced Options** section, check the **Sync with Workflow** option.
4. If you haven't already set up your Target Mappings for this attribute, follow the steps in Attribute Synchronization to do so.
5. **Save** your changes.

Customizing the Business Process for Attribute Synchronization

With Lifecycle Manager, IdentityIQ provides a standard business process for attribute synchronization; you can modify this business process according to your business needs. If you don't have Lifecycle Manager implemented, or if you prefer to use a completely custom business process, you can develop your own business process for attribute synchronization.

1. Click **Setup > Business Processes.**
2. Click the **Attribute Sync** business process to select it.
3. You can modify most of the details of this business process; the ones you are most likely to want to modify are the **Process Variables**:
    - **Approvals** can be enabled or disabled in the Approval section. If Approvals are enabled, you can choose who is responsible for approving requested attribute changes.

- **Notifications** can be enabled or disabled. When they are enabled you can select who should be notified when attribute changes are completed.

See the **Business Processes** documentation for more information.

Auditing Attribute Synchronization

If you want the ability to audit details about attribute synchronization, such as what triggered the synchronization, or which attributes were synchronized to which target systems, use IdentityIQ's Audit Configuration to enable auditing for this activity:

1. Click **gear > Global Settings > Audit Configuration.**
2. On the **General Actions** tab, check the box for **Attribute Sync**.
3. **Save** your changes.

To view audit details for attribute synchronization activity:

1. Click **Intelligence > Advanced Analytics.**
2. In the **Search Type** dropdown, choose **Audit**.
3. In the **Action** field under **Audit Attributes**, choose **attributeSync**. Note that attributeSync will not be available as a choice in this list unless there is attribute synchronization activity that has been completed in your system.
4. Enter any other search criteria you want to use.
5. Click **Run Search**.

Summary of Workflows, Tasks, and Rules in Provisioning

The following table provides an at-a-glance list of workflows, tasks and rules for provisioning through IdentityIQ.

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

Type	Name	Purpose / Usage
Workflow	Lifecycle Manager: LCM Provisioning LCM Create and Update LCM Manage Passwords LCM Registration	Manages actions requested through Lifecycle Manager.
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 can contain provisioning actions.
Workflow (subprocess)	Do Provisioning Forms	Creates, presents and gathers data from provisioning forms. This step is the interactive provisioning policy phase of provisioning.
Workflow (subprocess)	Do Manual Actions	Presents the unmanaged portion of a provisioning project as work items to be processed manually. Update and Identity Refresh workflows use this step. Lifecycle Manager has a similar step but audits differently.
Workflow (sub-	Provision with	Manages retries on the provisioning actions for Lifecycle Manager.

Type	Name	Purpose / Usage
process)	Retries	
Workflow (sub-process)	Identity Request Initialize Identity Request Violation Review Identity Request Approve Identity Request Approve Identity Changes Identity Request Provision Identity Request Notify Identity Request Finalize Provisioning Approval Sub-process	These workflows subdivide Lifecycle Manager Provisioning into more manageable workflow parts. LIfecycle workflows also use some or all of these tasks.
Task	Identity Refresh	Creates provisioning requests based on application of role assignment rules or role detection.
Task	Perform Maintenance	Processes certification-generated and policy violation-generated remediation requests.
Task	Account Aggregation	Provisioning activities driven by integration configurations or Work Items require a re-aggregation from the target system before the identities can be updated with the access change.
Rule	FieldValue	Identifies the default value for the Provisioning Policy field.
Rule	AllowedValues	Constrains allowed values for the Provisioning Policy field.
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 the triggering of a Lifecycle Event.