SailPoint - IdentityIQ

Introducing IdentityIQ

SailPoint IdentityIQ provides:

- Operational efficiency
- Integration with existing systems
- Access to all your identities
- Compliance to enterprises with complex environments

Benefits

- Stregthen security and lower risk
- Improve compliance and audit performance
- Deliver fast, efficient access for the business

IdentityIQ Capabilities

IdentityIQ Compliance Manager and **Lifecycle Manager** modules provide access management for the applications used by an enterprise and they share:

- Data and Database (Application Access Data)
- User Interface
- Implementation process

Integrated solutions instead have separate:

- Databases
- User Interface
- Implementation processes
- AI-Driven Identity Security (discover, manage, and control all your access-related data using machine learning and data intelligence)
- File Access Manager (helps locate and secure sensitive data, meet data privacy requirements and certify data access)

Lifecycle Management

- Flexible approval model
- Policy enforcement
- Automated lifecycle event management (as user join the company, switch roles, or leave)
- Batch updates (allow an IT team to make changes fo a set of users)
- Automated provisioning to connected applications

Compliance Management

- Functionality for applying security standards
- User's access control

- Policy scanning and violation detection

Identities: Core of Security

> **Identities** represent the users who have access to your corporate system and data. They include anyone or anything that has access to your enterprise systems, including employees, contractors, partners, even robotic users.

IdentityIQ represents each user with an **Identity cube**. It stores all the data collected and used by IdentityIQ for a single user, including identity attributes, enterprise accounts, and type of access held by the user.

Attribute

A property of an identity, account, application, or entitlment. Attributes often drive IdentityIQ processes. For example, a user's location may be used to give them application access.

Entitlement

Also known as **permissions**, are the type of access a user has when logging into an application.

Aggregation

The process of collecting or **reading** data from applications in your organization. Regular, periodic aggregation is key to keeping identity cubes up to date.

Governance Model Steps

1. **Aggregation**: Process of collecting data from the applications in your origanization, the key to keeping identities up-to-date
2. **Compliance Management**: With this module, the enterprise can confirm that the users have onlty the access they need
3. **Lifecycle Management**: Changes management to identities over time

Access Request

Users can ask for changes to access by requesting the addition or removal of roles and entitlements. Access requests are a function of the IdentityIQ Lifecycle Manager module.

Event-Driven Provisioning

> **Event-driven provisioning** is an automated process used to keep an identity's access current with their job needs and responsibilities. With it, enterprises can automatically provision or change access that’s required and remove access that's no longer necessary.

Event-Driven Provisioning Process

- IdentityIQ monitors data: looking for changes, also known as **events**
- IdentityIQ detects changes: when an event, or change, is detected by IdentityIQ, provisioning is initiated

- IdentityIQ provisioning data: the changes are written to the systems or applications that are defined to IdenitityIQ

Certification and Access Reviews

> **Certification**, also called access certification, is the process of collecting and reviewing the access that identities hold on IT-controlled systems in your organization.

During the certification process, a user's set of access is reviewed by certifier, often a manager or application or entitlement owner. The certifier makes the decision to approve or reject the access that a user currently holds. Certifications should be performed regularly, such as quarterly or annually, to ensure users have only the access they need.

Certification Steps

Steps of a sample manager certification campaign:

1. A certification campaign is created

   A compliance officer creates a manager certification campaign to require all managers to review and certify the access of their direct reports. The campaign creator also specifies when the campaign will run, how long it will last, and other key dates.

2. Access information is collected

   IdentityIQ collects and compiles all the required information related to identities, points of access, applications, and more. This process can take minutes, hours, or even days depending on the size of the campaign.

3. Access reviews are created for certifier review

   During the generation phase, an access review is created for each certifier designated in the certification campaign, and you can configure IdentityIQ to notify the certifiers that they have access reviews awaiting their action. A typical certification campaign may require certifiers to complete their reviews in a 2 or 4 week timeframe.

4. Each manager approves or revokes access

   Managers open their assigned access reviews and approve or revoke access for their employees. If AI-Driven Access Recommendations is deployed in the organization, managers will see a suggestion, based on comparisons with other identities, for each access.

5. Challenge, sign-off, and revocation

   An optional challenge phase allows users who would lose access to challenge that decision, and certifiers can reconsider their decisions.

   Once finalized, the managers sign-off on the access review, then IdentityIQ begins the revocation process, as needed.

Policies

> An IdentityIQ policy defines user access conditions that are unwanted by the organization. IdentityIQ policies define the access business policies of your enterprise. First, you define a policy, then IdentityIQ can prevent that condition from occurring or check the identities for that condition.

Separation of duties (SoD)

SoD policies ensure that users do not hold conflicting access; these policies are very common in many organizations. Generally, SoD policies ensure that no single user has access or responsibility for entire process, such as approving new vendors and also paying those vendors.

Dormant accounts

Accounts that are unused for excessive lengths of time, can lead to two problems:

- They can cost an organization money for application accounts that aren't being used and they can become a security risk
- If no one is using an account, no one will notice if it is compromised

Acting on Violations

The person assigned as the violation owner can take action on the violation through an assigned work item. Depending upon the type of violation, there are three possible actions that the owner can take:

- Allow it
- Correct it
- Certify the identity. Administrators have this option, which allows them to take a look at all access held by the user and make decisions about that access

A key purpose of the policy detection process is to ensure that someone is aware of undesired access and can take action to fix the problem. Once you've seen the violation, you can take steps to address it, which may involve actions outside of IdentityIQ. In IdentityIQ, you can allow the violation as an exception for a certain period of time. If the problem still exists after that time period ends, IdentityIQ will flag it again so it isn't forgotten.

Analytics and Reports

Advanced Analytics

IdentityIQ's powerful search mechanism is called Advanced Analytics. This feature allows you to easily search the IdentityIQ database. Search options will vary according to the configuration of IdentityIQ. For example, only attributes designated as searchable, will appear for selection.

The results can be viewed in IdentityIQ, saved for future searches, saved as a report, or exported as a CSV file.

The **identity search** is the most common type of search but there are many types of searches you can perform, including activity, role, entitlement, and audit.

IdentityIQ Reports

IdentityIQ reports provide up-to-date information to meet compliance needs and ease decision-making for your implementation.

IdentityIQ provides over 50 standard report options, organized by category, to display your data in a variety of meaningful ways, minimizing the need to manually search for information. Standard reports can be run without making any changes, or they can be configured to meet your specific needs.

Roles

> A **role** is a collection of one or more entitlements (permissions) encapsulated into a single object.

IdentityIQ Roles

In IdentityIQ, roles provide a way to define access for an individual. IdentityIQ provides a robust role model and role types to help model the access of users in your organization.

While roles are not required in IdentityIQ, they are beneficial in two significant ways:

- Increased efficiency
- Reduced risk

Increase Efficiency

When you use a role to group individual entitlements, you ensure that every time an interaction, such as a request or access review, occurs, users are dealing with one role instead of numerous entitlements. This increases the efficiency of items like access requests and approval and access reviews

Reduce Risk

If users must work with many individual entitlements, it's easier to make a mistake and request or approve inappropriate access. Managers may not be aware of which exact entitlements are required by employees. Working with a single role decreases the chances that they will request or approve more access than is necessary.

Automatic Role Assignment

Roles can be automatically assigned to users based on a rule. An assignment rule will commonly match an attribute of the identity, like a department or job title, with the attribute specified in the rule.

If the user's job title changes, IdentityIQ will recognize that his job title no longer matches the rule, and the role and its entitlements will be de-provisioned.

Role Modeling Options

Roles are typically modeled, built, and maintained by business analysts working in conjunction with application owners and business teams.

Extending IdentityIQ

IdentityIQ’s robust functionality can be extended to meet the needs of businesses that have complex processes, detailed data requirements, and stringent industry regulations. There are multiple levels for

extension.

Extended Attributes

All implementations include extended attributes, such as department, location, job title. These are data that your enterprise needs to manage your identity access program.

Rules & Branding

Most implementations use rules, little snippets of code injected into the IdentityIQ logic. Most will also brand IdentityIQ with their own colors and logos.

Workflows

While the workflows shipped with IdentityIQ provide many configuration options, many implementations will also include custom workflows.

Quicklinks

Some implementations add their own Quicklinks that can trigger a custom workflow to meet business-specific needs.

Custom Connectors

While SailPoint provides over 100 connectors, you may have specialized systems or home-grown applications that require a custom connector.

More on extended attributes

Extended attributes are essential for a robust IdentityIQ implementation. These attributes are *your* organization's important data – data that allows you to run your identity and access management program. These often include job titles, locations, and department names. Extended attributes add *implementation-specific* information to IdentityIQ objects.

Extended attributes drive IdentityIQ functionality and automated processes. Extended attributes can also be critical to provisioning processes; they can be examined when checking for policy violations and more.

- Standard attributes: The standard attributes are automatically included for each identity cube
- Extended attributes: Extended attributes are specific to each implementation (department, location, ID, job title etc)

When extended attributes are added to the system, the implementer can choose to designate them as **searchable**. Those that are searchable are automatically added to options throughout IdentityIQ.

Other objects to extend

There are six objects to which extended attributes can added. In addition to identity cubes, there include:

- Entitlements
- Roles
- Applications

- Accounts
- Certifications

IdentityIQ Plugins

A **plugin** is a software component that adds functionality to an existing program. You can use them to extend IdentityIQ functionality.

Plugins can be downloaded from Compass, and many SailPoint partners also provide IdentityIQ plugins. Examples include:

- A support plugin developed by SailPoint helps collect data from your IdentityIQ instance and provides it to the SailPoint support team. The plugin collects the required data into one zip file for uploading.
- The SQL Browser Tool provides administrators with view-only access to the IdentityIQ database to help implement and support IdentityIQ.