A Smarter Way to Manage Identity

COMPLIANCE MANAGER
LIFECYCLE MANAGER
ACCESS MANAGER
IDENTITY INTELLIGENCE
GOVERNANCE PLATFORM
CONNECTIVITY FOUNDATION
“SailPoint is competing — and winning — against some very large companies in the identity management market because of our innovative products, and our unmatched commitment to helping companies succeed with their compliance and security efforts. We’re very focused on maintaining our high customer satisfaction levels, and have invested a significant amount of resources internally to make that possible.”

MARK MCCLAIN, CEO AND FOUNDER, SAILPOINT
Overview

A Smarter Way to Manage Identity
Managing access to information in today’s dynamic, data-driven environment is a challenge, to say the very least — and one that requires much more from identity and access management (IAM) solutions than ever before. To be effective, these solutions must deliver access to all the applications and information that business users need, when they need it, from wherever they need it — while at the same time ensuring enterprise security policies are consistently enforced. And they must provide the transparency and proof of strong controls required to satisfy audit and compliance requirements.

SailPoint IdentityIQ™ is a complete governance-based identity and access management solution that provides fast, convenient application access that keeps business users productive, and access controls that keep the business safe.

IdentityIQ integrates governance, provisioning and access management into a unified solution that leverages a common identity governance framework. Because of this approach, IdentityIQ consistently applies business and security policy and role and risk models across all IAM activities.

SailPoint IdentityIQ enables organizations to:
- Manage compliance using automated access certifications and policy management
- Empower users to request access and reset passwords independently
- Automate provisioning across the user lifecycle by simplifying processes for creating, modifying and revoking access
- Enable secure, yet convenient access to any application, from any device
- Provide on-demand visibility into “who has access to what” to help make business decisions and meet audit requirements
- Enable users to easily sign-on to web and SaaS applications without having to remember multiple passwords
- Gain more visibility into all user access from the datacenter to the cloud and proactively enforce risk-appropriate governance controls
- Make a smooth transition from on-premises IAM to IAM-as-a-Service (IDaaS) if and when the time is right

“CUNA Mutual wanted to improve the accuracy and efficiency of access certification and more efficiently control the provisioning and de-provisioning processes. SailPoint IdentityIQ was the obvious choice because it delivered identity governance and provisioning capabilities in a single solution. It was also immediately evident that it would be easy for our business managers to use, and provided us insight into the risk associated with user access.”

Director of Information Security, CUNA Mutual
IdentityIQ Solution Components

SailPoint IdentityIQ is the only IAM solution built from the ground up as a fully integrated IAM solution. It leverages a unified governance platform to provide a common data repository and role, policy and risk model — giving you a solution that’s easier to deploy, easier to maintain and easier to use. The key components of IdentityIQ include:

- **Compliance Manager** — Streamlines compliance controls and improves audit performance through automated access certifications and policy management.
- **Lifecycle Manager** — Combines self-service access request and password capabilities with automated lifecycle event management which simplifies creating, changing, and revoking user access privileges based on user lifecycle changes.
- **Access Manager** — Offers governance-based single sign-on (SSO) to cloud, on-premises web, and mobile applications through easy-to-use desktop and mobile interfaces.
- **Identity Intelligence** — Highlights business-relevant information in easy to understand dashboards, reports and advanced analytics.
- **Governance Platform** — Centralizes identity data and provides a single place to model roles, policies, and risk to support compliance, provisioning, and access management processes across the organization.
- **Connectivity Foundation** — Provides flexible options for connecting to enterprise and cloud resources to aggregate identity data and orchestrate changes resulting from compliance and provisioning processes.

*Within 90 days of the IdentityIQ project commencing, ING DIRECT Australia was able to improve the compliance processes associated with executing a certification cycle by 98% — from 184 hours and two staff members to 4 hours and one staff member.*

**ING Direct**

**Compliance Manager**

IdentityIQ Compliance Manager enables the business to streamline compliance processes for greater effectiveness while lowering costs. By integrating access certification and policy management, Compliance Manager automates the auditing, reporting and management activities associated with a strong identity governance program in the datacenter and the cloud.

**Access Certifications**

Many organizations struggle to implement an effective access certification process that ensures a user’s access privileges match the requirements of his or her job function. IdentityIQ provides a fully automated, repeatable certification process and tracks and reports on the status of certifications by individual, application and organizational groups. IdentityIQ automates all access certification tasks including formatting of user

---

**ACCESS CERTIFICATION IN ACTION**

Compliance Manager delivers visibility and control over enterprise access. Annotating certification reports with descriptive business language and other helpful information to highlight changes and flag anomalies enables reviewers to focus on areas of potential risk and make better decisions.
role and entitlement data into easy-to-read, business-oriented reports; routing of reports to the appropriate reviewers; tracking reviewer progress and actions; and archiving certification reports and data.

To make the reviews more effective, IdentityIQ uses descriptive business language in reports and provides helpful information highlighting changes and flagging anomalies so that reviewers are better equipped to mitigate areas of potential risk and make better decisions. To enhance transparency of certification activity across the organization, compliance administrators have access to real-time information about the status of individual certifications from dashboards, reports and analytics.

**Policy Management**
Defining and enforcing comprehensive access policy across enterprise applications is critical to implementing strong compliance controls. IdentityIQ makes it easy for business and IT managers to define access policy across roles and entitlements using point-and-click interfaces. Compliance Manager validates users’ existing access privileges against a wide variety of policy types, including entitlement and role separation-of-duty (SoD) policies, application/account-based policies, activity policies and risk-based policies.

It automatically scans identity data for policy violations and can be configured to alert business and IT managers, immediately revoke access, or run a pre-defined business process. In addition, policy violations can be resolved directly — through a user-friendly interface designed for reviewing and mitigating violations — or as part of an access certification where violations are highlighted for review and resolution by the certifier. IdentityIQ tracks the status of policy violations, incorporating this information into identity risk scores, reports and compliance dashboards. Managers can lower risk scores by revoking access that results in a policy violation or by explicitly allowing an exception for a predetermined period of time.

**Audit Reporting**
Compliance Manager enables compliance administrators, auditors and business managers to get the information they need on-demand from reports and personalized dashboards — with data presented in a simple to use, business-friendly format. Compliance Manager also provides advanced analytics that allow for direct, customized queries, along with integration to third-party reporting and GRC tools.

**Lifecycle Manager**
IdentityIQ Lifecycle Manager delivers a business-oriented solution for managing changes to user access, including self-service requests, password changes and resets, and automatic event-driven changes. By combining self-services tools for the business, with automated user provisioning driven by IT, Lifecycle Manager helps keep access aligned with a constantly changing world.

**Self-Service Access Request**
Lifecycle Manager provides a user-friendly solution for managing access requests. Users are guided to the right access through the IdentityIQ Request Advisor, which leverages Google-like keyword search and affinity-based search options that locate privileges based on what other business users have. Once users have selected access to request, they can review their shopping cart and check out using an intuitive e-commerce interface.

Governance is enforced throughout the access request process via configurable policy checking and approval workflows. In addition, organizations can leverage the IdentityIQ risk model to increase scrutiny of high-risk access changes.

**Password Management**
With Lifecycle Manager, users can self-manage passwords from its business-friendly interface, greatly reducing calls to the help desk and IT support. End users can automatically change passwords across multiple systems or recover forgotten passwords by correctly
answering challenge/response questions, and managers and administrators can reset end user passwords.

To improve application security and reduce risk, Lifecycle Manager automatically enforces application-specific password policies. Password changes are automatically synchronized with target systems through the IdentityIQ connectors or integration with third-party provisioning solutions.

**Lifecycle Event Management**

Managing workforce churn and the resulting impact to identities and access privileges is greatly simplified in IdentityIQ with automated lifecycle events. Lifecycle Manager supports a wide range of joiner, mover, leaver events such as new hires, transfers, moves or terminations through integration with authoritative sources, such as HR systems and corporate directories.

When a lifecycle event is detected, IdentityIQ automatically triggers access changes by initiating the appropriate business process, including policy checks and approvals. Changes are then passed to the Provisioning Broker for closed-loop access fulfillment via IdentityIQ’s connectors, 3rd party provisioning systems or manual change management. By automating access changes triggered from identity lifecycle events, IdentityIQ greatly reduces the costs associated with managing those changes while enhancing the organization’s security and compliance posture.

**Access Manager**

IdentityIQ Access Manager empowers users with single sign-on (SSO) to cloud and web applications from any device — at work, home or on the go. And it enables IT to effectively apply security policy, detect violations and ensure regulatory compliance. Application usage visibility also helps monitor monthly subscription expenses by promptly deprovisioning unused or unauthorized cloud application accounts.

**Single Sign-On (SSO)**

IdentityIQ Access Manager eliminates the need for users to remember and enter multiple user names and passwords. It delivers a consistent and convenient SSO experience for the applications that users use every day. This includes seamless, password-free SSO to all internal web apps via a reverse-proxy virtual appliance server and to third-party software-as-a-service (SaaS) applications that support federation standards. Users also gain the benefit of SSO for self-provisioned (“Bring Your Own”) apps or third-party services that don’t support SSO standards, freeing them from the burden of remembering and continually entering passwords throughout the day. Access Manager also provides convenient SSO from mobile devices using the same security and credentials as from the desktop.

**Strong Authentication and Policy-based Controls**

Because Access Manager is part of the IdentityIQ integrated suite, it leverages enterprise-wide policy and control information to make access management decisions smarter. Critical information such as high-risk users or highly sensitive access permissions enable Access Manager to enforce strong authentication where needed. Strong authentication mechanisms include a one-time password (OTP) sent to a user’s phone; knowledge-based authentication (KBA) consisting of challenge/response questions; or integration with third-party strong authentication tools, such as smartcards or OTP tokens.

To ensure that users are complying with security policies and not putting the company at risk, Access Manager utilizes application usage agreements to educate users about appropriate use policies (especially self-provisioned “BYOA” apps) and to capture auditable acknowledgement that users will follow policy. Usage agreements can be displayed to users on a per-app basis before they access an application, and IdentityIQ creates an auditable record of the users’ responses.
Synchronized SSO and Provisioning
Access Manager provides an intuitive, self-service storefront that gives users a single, convenient place to find and request access to a broad catalog of business and personal applications — available to them on any device. When new access is requested, it can be automatically provisioned based on the user’s job function or role within the organization, via seamless integration with IdentityIQ Lifecycle Manager. The same approval processes and provisioning policies are automatically applied as for other access request services.

For SaaS applications or on-premises web applications that are licensed per user, Access Manager can monitor for accounts that are not regularly being used and issue alerts to managers to deactivate or automatically de-provision those accounts. Reducing unnecessary software costs is an added benefit of IdentityIQ’s integrated access management and provisioning solutions.

Identity Intelligence
With Identity Intelligence, organizations can transform technical identity data scattered across multiple enterprise systems into centralized, easily understood and business-relevant information. The visibility and insights offered by IdentityIQ through dashboards, risk metrics and reporting provide a clear understanding of identity and access information.

Reporting and Analytics
IdentityIQ provides business-friendly reports and analytics tools that make it easy to track and monitor critical metrics and processes. The reports offer powerful charting and graphing capabilities, and allow compliance and audit users to monitor and analyze the status of key compliance controls, including access certifications, policy violations, remediations and risk scores. IdentityIQ reports also provide real-time information to business and IT teams on lifecycle management and provisioning activities. IdentityIQ’s advanced analytics capabilities enable users to quickly create customized queries using a point-and-click interface. Each query can be saved as a report for easy recall. Direct connect options also allow organizations to leverage third-party business intelligence and GRC tools on top of IdentityIQ’s data model.

Dashboards
The IdentityIQ dashboard simplifies how business users manage access, with features like one-click entry into access request, password management and compliance activities. “Visual alerts” highlight actions that need to be taken, such as approvals, policy alerts and certification notifications. Business and IT users can personalize their dashboards with easy drag-and-drop formatting and content selection. The dashboard is interactive, allowing users to drill down to see more detailed source data.

**IDENTITY INTELLIGENCE IN ACTION**
Dashboards empower users with better visibility enabling them to conveniently drill down into the source data for more details or to view the status of pending tasks. Each user can easily tailor the dashboard to his or her level of sophistication, as well as his or her role and authority.
Governance Platform
The IdentityIQ Governance Platform lays the foundation for effective identity and access management by centralizing identity data and establishing a consistent policy, role and risk model that is used across all IdentityIQ components.

Identity Warehouse
The Identity Warehouse serves as the central repository for identity and access data across all enterprise IT applications in the datacenter and the cloud. The warehouse is populated by importing user data from authoritative sources, business applications, databases, platforms, and SaaS applications, leveraging out-of-the-box connectors or flat file extracts. During the import process, IdentityIQ leverages a powerful correlation engine to link individual accounts and entitlements to create a user’s Identity Cube — a multi-dimensional view of each individual users and their associated access.

Policy Model
The IdentityIQ Policy Model provides a highly extensible framework for defining and implementing both detective and preventive audit controls, and spans several policy types: governance, access request and provisioning. Common governance policies regulate and control the access privileges users are allowed to possess within the organization based on their job function, i.e., separation-of-duty (SoD) rules. Access request policies establish rules for who and what can be requested and who can approve, and provisioning policies define the change fulfillment process. In addition, the Policy Model defines and reuses enterprise access policies across business applications and organizational business processes in the datacenter and in the cloud.

Role Model
By allowing organizations to request, approve, define policy and certify access using business roles rather than low-level technical entitlements, the IdentityIQ Role Model reduces complexity and simplifies user administration while enforcing “least privileged” access. With a combination of top-down, business-oriented role mining and bottom-up IT role mining, business and technical users can quickly create roles that accurately reflect the organization’s business and IT requirements. Once the role model is created, the Role Modeler ensures it stays in sync with organizational and IT changes. IdentityIQ provides end-to-end role lifecycle management capabilities including automated role approvals, role certifications, role quality metrics and role analytics, including what-if analysis to see how proposed changes will impact users before changes are implemented.

Risk Model
The Risk Model locates and identifies areas of risk created by users with inappropriate or excessive access privileges. It provides a dynamic risk model, for both users and applications, which leverages patent-pending risk algorithms to calculate and assign a unique identity risk score for each user, application and system resource. The risk score is updated continuously based on changes to the user’s access privileges, as well as “compensating factors,” such as how recently the user has been certified and whether a policy violation has been allowed as an exception. By leveraging risk scores, managers and application owners can target the highest-risk users or systems first, improving the effectiveness of controls for their departments and, ultimately, the security and compliance of the business.
Connectivity Foundation
IdentityIQ provides a flexible Connectivity Foundation with pre-built integration to over 80 cloud and on-premises resources, along with integration options for other provisioning vehicles, such as third-party provisioning tools, service desk systems, and even manual provisioning processes. IdentityIQ seamlessly orchestrates how changes get fulfilled across multiple fulfillment mechanisms, giving organizations maximum flexibility to provision changes in whatever way they choose.

Cloud and On-Premises Resource Connectors
IdentityIQ provides pre-packaged integration with platforms, databases, directories, and business applications running in the datacenter or in the cloud. Resource connectors speed loading of data into the Identity Warehouse and automate provisioning of account and password changes. The solution also includes a connector toolkit for rapidly building and deploying connectors to custom applications.

Cloud Gateway
The Cloud Gateway simplifies management and control over applications deployed in public or private cloud environments. It also allows customers or partners to host IdentityIQ in the cloud and seamlessly connect to on-premises resources. The Cloud Gateway synchronizes access changes over a secure, encrypted connection between IdentityIQ and enterprise systems in different networks. It deploys as a virtual appliance to reduce administration and maintenance requirements.

Third-Party Provisioning Integration
SailPoint recognizes that many organizations have significant investments in legacy provisioning systems. To maximize existing investments in these systems, SailPoint offers Provisioning Integration Modules (PIMs) for BMC Identity Manager, IBM Security Identity Manager, IBM Tivoli Directory Integrator, Novell Identity Manager, Oracle Identity Manager and Sun Identity Manager. IdentityIQ leverages PIMs to pull user account data into its Identity Warehouse and to route access changes to third-party provisioning solutions for fulfillment.

Service Desk Integration and Work Queues
IdentityIQ supports several options for manually making changes to user access through help desks and work queues. Service Desk Integration Modules (SIMs) automatically generate help desk tickets when access needs to change on a target resource. SIMs are available for common service desk applications including BMC Remedy and ServiceNow. Internal work queue management supports the creation and tracking of internal work items for changes that need to be fulfilled through manual provisioning processes.
## SailPoint IdentityIQ Key Capabilities

### Compliance Manager

<table>
<thead>
<tr>
<th>CAPABILITY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| **Access Certifications**      | • Automate access review cycles with flexible scheduling options  
• Present data in business-friendly language  
• Focus reviewers on exceptions and high-risk items  
• Track reviewer progress and actions  
• Enforce a closed-loop provisioning process |
| **Policy Management**           | • Enforce multiple types of access policy across cloud and on-premises applications  
• Proactively detect and prevent inappropriate access and violations in real-time  
• Prioritize violation response with risk-based approach  
• Track and report on violations |
| **Audit Reporting**             | • Highlight effectiveness of compliance controls  
• Track compliance performance through a simple enterprise-wide dashboard  
• Archive certification and policy violation history |

### Lifecycle Manager

<table>
<thead>
<tr>
<th>CAPABILITY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| **Self-Service Access Request** | • Empower users to request and manage access using an e-commerce shopping experience  
• Help business users find the right access with keyword and affinity search features  
• Facilitate delegated administration by managers and help desk/admins  
• Provide visibility to request status and process execution |
| **Password Management**         | • Allow business users to change and reset passwords  
• Automatically detect and synchronize passwords  
• Enable delegated password management by managers and help desk/admins  
• Enforce strong password policies |
| **Lifecycle Event Management**  | • Automate access changes based on HR lifecycle events (i.e., hires, transfers, terminations)  
• Prevent policy violations and consistently enforce the desired state  
• Orchestrate changes across automated and manual provisioning processes  
• Gain complete visibility to process execution |

### Access Manager

<table>
<thead>
<tr>
<th>CAPABILITY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| **Single Sign-on (SSO)**                      | • Eliminate the need for users to remember and enter multiple user names and passwords for SaaS apps, internal web apps, and mobile apps  
• Provide convenient SSO from mobile devices using the same security and credentials as from the desktop |
| **Strong Authentication and Policy-based Controls** | • Enforce strong authentication to apps based on identity risk, such as role membership, privileged account ownership, or risk score  
• Provide strong authentication via a one-time password (OTP) sent to a user’s phone or knowledge-based authentication (KBA) consisting of challenge/response questions  
• Support integration with third-party strong authentication tools, such as smartcards or OTP tokens  
• Educate users on appropriate terms of use policy and capture their acknowledgement as audit events |
| **Synchronized SSO and Provisioning**         | • Provide convenient App Store to add new applications to SSO Launchpad  
• Provision access to applications using the same policies and approval processes as for other IT services  
• Identify unused or unauthorized accounts and reports them back to the appropriate business sponsor for removal and potential cost savings |
### Identity Intelligence

<table>
<thead>
<tr>
<th>CAPABILITY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Reporting and Analytics        | • Access predefined reports for compliance, provisioning and access management  
• Leverage report designer for custom reporting requirements  
• Gain needed information on-demand with powerful advanced search capabilities |
| Personalized Dashboards        | • Notify users of required actions with “visual alerts”  
• Provide one-click entry into access request, password management and compliance activities  
• Deliver at-a-glance charts, graphs and reports with drill-down capabilities  
• Highlight scheduled compliance events and the status of in-process tasks |

### Governance Platform

<table>
<thead>
<tr>
<th>CAPABILITY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Identity Warehouse             | • Leverage single system of record for identity data across all IAM functions and activities  
• Import data using out-of-the-box connectors or via flat files |
| Policy Model                   | • Define and implement detective and preventive controls with compliance, access request and provisioning policies  
• Proactively identify and route violations for review or immediate revocation |
| Role Model                     | • Define flexible role types that enforce “least privilege” access  
• Discover business and IT roles based on identity attributes and entitlements  
• Provide automated role approvals, role certifications, role quality metrics and role analytics  
• Use “what-if” analysis to see impact of changes before they are implemented |
| Risk Model                     | • Locate and identify areas of risk across users and applications  
• Calculate and assign unique identity risk score  
• Continuously update risk scores based on changes to user access |

### Connectivity Foundation

<table>
<thead>
<tr>
<th>CAPABILITY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Cloud and On-premises Resource Connectors | • Speed provisioning of access changes to managed resources on-premises and in the cloud with over 80 out of the box connectors  
• Support rapid deployment to custom applications |
| Cloud Gateway                  | • Extend identity and access management capabilities to public/private cloud environments or host IdentityIQ in the cloud and connect to datacenter applications |
| Third-Party Provisioning Integration | • Leverage third party provisioning solutions to import data or provision changes to target systems |
| Service Desk Integration and Work Queues | • Generate help desk tickets or manual work items to fulfill access changes |
Industry-leading Enterprise IAM for Today's Hybrid IT Environments

SailPoint IdentityIQ provides a unified approach across core IAM activities leveraging a common identity governance framework to provide the industry’s richest set of controls spanning the datacenter to the cloud.

IAM Services and Solution Modules

- Single Sign-On
- Password Management
- Access Certification
- Access Request & Provisioning
- Advanced Policy & Analytics

Compliance Manager  Lifecycle Manager  Access Manager

Unified Governance Platform

- Policy Model
- Role Model
- Identity Warehouse
- Risk Model
- Workflow Engine

Open Connectivity Foundation

- Resource Connectors
- Provisioning Integration
- Service Desk Integration
- Cloud Gateway

Column Technologies

Column Technologies is a global technology solutions provider and the preferred managed services partner for SailPoint IdentityIQ. The products and services are centered around IT Management, information security, and consulting services that reflect the experience of over 3,000+ IT management implementations worldwide.

About SailPoint

As the fastest-growing, independent identity and access management (IAM) provider, SailPoint helps hundreds of the world's largest organizations securely and effectively deliver and manage user access from any device to data and applications residing in the datacenter, on mobile devices, and in the cloud. The company's innovative product portfolio offers customers an integrated set of core services including identity governance, provisioning, and access management delivered on-premises or from the cloud (IAM-as-a-service). For more information, visit www.sailpoint.com.

© 2014 SailPoint Technologies, Inc. All rights reserved. SailPoint, the SailPoint logo and all techniques are trademarks or registered trademarks of SailPoint Technologies, Inc. in the U.S. and/or other countries. All other products or services are trademarks of their respective companies. 0914-4294