

The Why and How Organizations Should Migrate from SailPoint IdentityIQ to SailPoint Identity Security Cloud

Why Organizations Should Migrate to the SailPoint Identity Security Cloud Platform

SailPoint has been a leading identity security solutions provider for almost 20 years, with its flagship software-based solution, IdentityIQ, placing it at the top of the leaderboard. SailPoint remains committed to portfolio updates to better serve their customers, so with the release of the SailPoint Identity Security Cloud Platform including IdentityNow (IDN), it is no surprise to us that identity professionals are taking notice of this purpose-built, intelligent, autonomous identity solution and wondering “if”, “why” and “how” they should migrate to it.

The Sailpoint IdentityIQ (IIQ) Flexibility Conundrum

In addition to the numerous identity security features IdentityIQ has to offer, one unintended but notable benefit is a flexible customization feature. SailPoint IdentityIQ is a lightweight, java-based web application software that implementors quickly discovered they could easily deploy and customize in almost any environment.

As a result, SailPoint IdentityIQ implementors routinely take advantage of this flexibility and apply heavy customizations on components and internal core libraries and objects, exploiting a feature IdentityIQ was never intended to perform. SailPoint never supported the customization of internal core libraries and, in response, published warnings aimed at discouraging implementors from this practice.

The High Cost of Maintenance

Like all on-premises based applications, the responsibility of maintaining the SailPoint IdentityIQ environment is the sole responsibility of the owner. In addition to regular enhancement and customization deployments, timely patching and upgrades are also critical to ensure the IdentityIQ environment remains bug free and secure.

Unfortunately, applying patches and upgrades to a heavily customized IdentityIQ environment can quickly turn regular, periodic planning, application, and sanity testing into a cumbersome and time-consuming process that year-over-year increases maintenance costs.

IdentityIQ Customers who have over-exploited the customization feature are now finding themselves facing a large and expensive maintenance burden that they need to resolve and a good bit of confusion about how to proceed. Due to the inherent risk of the platform failing when discarding the customizations, the obvious solution of choice for those organizations struggling is to migrate to a completely different solution.

THE SAILPOINT IDENTITY SECURITY CLOUD PLATFORM SOLUTION

The SailPoint Identity Security Cloud Platform is a SaaS-based program with the flexibility to safely and confidently add-on additional SaaS identity security capabilities. SailPoint’s unique offer to “bundle” identity security requirements delivers organizations – including new and existing SailPoint IdentityIQ on premises software users – a more customized approach to identity security and negates the high maintenance and costs associated with IdentityIQ customizations.

With all the benefits of a SaaS based deployment model, including availability, extensibility, and scalability, the SailPoint Identity Security Cloud Platform also comes equipped with its own unique set of identity features and capabilities not found in any other SaaS offering or software-based solution, these features include:

1. AI Driven Access Insights and Recommendations for highlighting actionable identity data and associated potential risks, making informed intelligent decisions to accelerate certifications and access request process.
2. Cloud Governance for IaaS decisions and SaaS Management for governing access on SaaS based integrated applications.
3. Add-ons such as:
 - a. Non-Employee Risk Management
 - b. Access Risk Management
 - c. File Access Manager
 - d. Password Management

The entire deployment process is owned, managed, and maintained in the backend by SailPoint, and the platform offers fully supported, comprehensive integrations for third-party applications. Led by AI driven automation, integrations are frictionless, and typical IGA processes are more effective through optimizations, recommendations, and suggestions. The newly refreshed, user-friendly interface and features increase the user's overall productivity and meet the demand from organizations for higher operational efficiency.

SailPoint IdentityNow (IDN)

SailPoint IDN, a part of the suite of SailPoint Identity Security Cloud products, is the SaaS based counterpart to SailPoint IdentityIQ and is in no way less than IdentityIQ in terms of identity governance and administration (IGA) capabilities.

IdentityNow supports customizations with a certain degree of limitation built-in. Customizations available on the user interface (UI) can be safely deployed as extensions of the product after a simple SailPoint review-and-approve process. This process ensures that the organization's customizations do not exceed the underlying capabilities and ideology of the SailPoint IDN product.

In stark contrast to IdentityIQ's burdensome and expensive application maintenance, IdentityNow – and all other solutions offered within the SailPoint Identity Security Cloud Platform – provide a seamless deployment strategy of patches and upgrades at no additional cost. The responsibility of deployment of the patches and upgrades lies with SailPoint and is executed without disruption to service on the backend. Owners also have the flexibility to validate the upgrade and can either choose to keep it or revert to a previous state.

SDG'S APPROACH

How to Migrate to the SailPoint Identity Security Cloud Platform

SDG has 20+ years of experience in identity and access management which includes extensive knowledge of – and experience with – SailPoint's products. Our team is powered by highly qualified and certified IGA and SailPoint professionals who are committed to streamlining identity and access management controls.

SDG's keen focus on modern, sustainable identity programs for customers led to the creation of a set of pre-defined approaches for migrating to the SailPoint Identity Security Platform. Depending on the size, footprint, and complexity of the organization's existing IdentityIQ implementation, SDG works to advise and guide organizations through the best migration approach for its situation, whether that is a "Lift & Shift" or "Coexisting Transition" approach.

While the SailPoint Identity Security Cloud Platform with IdentityNow follows a similar object structure, features, and capabilities matrix as IdentityIQ, there are deviations that every organization should consider before planning their migration roadmap.

At SDG, we have identified the most common deviations and mapped them into key considerations organizations should regard before beginning migration to the SailPoint Identity Security Cloud Platform:

Features	Description	Remarks	Impact
QuickLinks & Forms	Custom QuickLinks & forms are heavily used for access request & provisioning	- Identity Security Cloud does not support custom QuickLinks & forms - Access would need to be modeled as roles/access profiles/entitlements	- Access requests & approvals - Application access profiles & policies - Access provisioning
Logical	Tired Application Simulations	- Identity Security Cloud does not support logical applications as supported in IdentityIQ - Logical applications access would need to be modeled as roles rather individual applications	- Access requests & approvals - Application access profiles & policies - Access provisioning
Loopback Connector	Delegated Administration	- Identity Security Cloud does not support loopback connector mechanism to manage/administer workgroups/capabilities as in IdentityIQ - Governance Groups can be used wherever feasible for access requests & reviews	Delegated Administration

Features	Description	Remarks	Impact
Workflows	Lifecycle management & access request workflows	• IdentityIQ supports customization, whereas Identity Security Cloud is more configurable driven	• Identity lifecycle management - joiner, leaver, LOA • Access requests & approvals
Rules	Conditional evaluation of business logic	• All the rules to be submitted for the review before putting in the instance • Rule review hours are capped at 10 hours a year. Additional support would be required to be purchased.	• All kind of rules to be reviewed and approved
Plugins	Custom feature and functionality built using plugin framework	• Identity Security Cloud does not support plugins	• Custom features & functionality

Recommendation:

- Redesign/Remodel access policies/profiles - move from form-based access requests to catalogue driven (entitlement/role) access requests.
- Leverage existing investments to streamline, simplify and modernize the life cycle management, access requests & provisioning.
- Laydown the foundation for seamless move to SaaS (SailPoint Identity Security Cloud) - evaluate & plan

Streamlining and Organizing Migration Efforts

Migrating from SailPoint IdentityIQ (IIQ) to SailPoint IDN involves careful planning and execution to ensure a seamless transition of identity governance capabilities. At SDG, we have come up with a roadmap with sequential step to streamline and organize the migration efforts at different stages of the journey:

1. Assessment and Planning

- a. Assess: Components, configurations, customizations.
- b. Plan: Migration objectives, scope, timelines, and budget.

2. Connector Analysis, Configuration and Customizations

- a. Identify: Connectors & integrations, Use Cases & Features, Business Process
- b. Evaluate: Customizations in IdentityIQ and assess their relevance in IdentityNow.

3. Data Cleanup and Pre-migration Activities

- a. Prepare: Cleanup of identity data in IdentityIQ, Re-design, optimize, streamline and discard of components & use cases in IIQ

4. Migration Strategy

- a. Select: Choose a migration strategy based on outcomes of previous steps.

5. Operations and Transitions: Depending upon outcome of previous steps, customers can choose to move forward with parallel “Coexisting Transition” or big-bang “Lift & Shift” migration approach

- a. Execute:
 - i. Shift all key components, configurations and integrations at once in IdentityNow and retire IdentityIQ
 OR
 - i. Run IdentityIQ and IdentityNow in parallel
 - ii. Gradually migrate components, configurations and integrations.

6. Data Migration

- a. Develop a data migration plan to transfer identity related data
- b. Execute the data migration in a controlled manner to minimize disruptions

7. Testing and Validation

- a. Validate: System integration Testing, Functional testing, User acceptance testing (UAT)

8. Training and User Adoption

- a. Handover: Provide training to administrators, certifiers, and end-users on how to use IdentityNow effectively

9. Post Migration Support

- a. Hypercare/MSS: Post-migration support to address any post-migration issues or challenges. System monitoring Health-check and optimizations.

To facilitate and accelerate the migration journey, we offer the following utilities:

Starter Packages



- Built to jump start migration
- Customized and tailored to our customer's unique IGA ecosystem and footprint.

Application Onboarding Factory



- Automation and agility for deploying high quality application integrations
- Optimize and streamline the onboarding process

Automation Tools



- Pre-built API-based utilities for faster migration of compatible and supported objects from IIQ to IDN

CONCLUSION

Organizations across the globe have spent years utilizing the unintended flexible customization IdentityIQ offers. However, as organizations scaled, so did the number of customizations, resulting in a burdensome process and high maintenance costs for regular enhancement and customization deployments, timely patching, and upgrades.

SDG, an experienced and respected SailPoint partner, works with organizations to migrate from IdentityIQ to the SailPoint Identity Security Cloud Platform swiftly, safely, and securely. We have the experienced team that can take full advantage of IDN's configurability to harmonize customizations where possible. SDG's seasoned experts provide the insight, guidance, and skills necessary to facilitate migration, expedite processes, accelerate the maturity of the organization's IAM program, and reduce costs.

ABOUT SDG

With more than 30 years of experience partnering with global enterprises on complex business and IT initiatives, SDG is a trusted provider of advisory, transformation, and managed services. The firm empowers organizations to strengthen cyber resilience by integrating AI into identity, threat, and risk management solutions that protect digital assets and deliver measurable business value. Learn more at www.sdgc.com.



Contact Us: solutions@sdgc.com

■ 75 North Water Street
Norwalk, CT 06854

■ 203.866.8886

■ sdgc.com