Streamline security and access control with SailPoint and Okta

KPMG Cloud Identity Governance Bridge

Cloud adoption continues moving rapidly upward. It is predicted that up to 40 percent of application software—including productivity apps and tools for customer relationship management (CRM), human capital management (HCM), supply chain management (SCM), and enterprise resource planning (ERP)—will move to the cloud by 2022.[1]

With enterprises shifting to cloud-based alternatives at increasing velocity, IT executives are charged with protecting critical data while also streamlining user access to these cloud applications. Yet, businesses are not running 100 percent on the cloud. On-premises applications must also be secure and accessible. Given today's reality of hybrid enterprise environments, IT executives need to deploy identity and access management (IAM) technology that responds to the unique needs of this hybrid reality.

KPMG can help integrate identity governance for both cloud and on-premises applications while streamlining IAM in a hybrid environment. Companies that use— or are considering using—SailPoint IdentityIQ and Okta can leverage KPMG Cloud Identity Governance Bridge to manage users, applications, accounts, and certification actions for both cloud and on-premises applications.

Enhanced security and control with KPMG, SailPoint, and Okta

KPMG's strategic alliances with SailPoint and Okta can help your company protect information and deliver secure access, even as you pursue new digital interactions and enhanced productivity in the cloud. KPMG provides the services and capabilities that enable enterprises using both SailPoint IdentityIQ and Okta to streamline and integrate their IAM strategies.

Transform your security with KPMG

KPMG's IAM and cybersecurity teams help clients conceptualize, design, implement, measure, and improve their information security programs as part of a broad, business-centric transformation program. A customized cyber strategy provides informed threat intelligence and alignment with your risk tolerance. KPMG can help you implement an identity management program to help minimize risk, address compliance requirements, enhance user experience, streamline business processes controls, and optimize user administration operations.

Leading IAM technology from SailPoint

SailPoint provides a detailed IAM platform that integrates access provisioning and compliance management under a single identity governance framework. Its flagship product, IdentityIQ, delivers access to applications and information within the corporate firewall. Business users can get the information they need, when they need it, from wherever they need it—while at the same time ensuring enterprise security policies are consistently enforced. IdentityIQ also addresses audit and compliance requirements by providing transparency of strong controls.

---

[1] Gartner Press Release, "Gartner Says 28 Percent of Spending in Key IT Segments Will Shift to the Cloud by 2020." September 18, 2018. Customer Relationship Management (CRM), Human Capital Management (HCM), Supply Chain Management (SCM), Enterprise Resource Planning (ERP)

Reliable security and access for cloud applications with Okta

Okta securely provisions and connects thousands of enterprise employees to cloud applications every day. Its platform, Okta Cloud Identity, provides single sign-on (SSO) capabilities for thousands of pre-integrated cloud applications; risk-based, multifactor authentication for accessing cloud services outside the corporate firewall; and automated provisioning to easily create accounts for new employees. The technology provides a user-friendly way for your employees to access their applications, tailored to each device, and is customizable.

KPMG's capability for digital identity leveraging Okta and SailPoint

KPMG Cloud Identity Governance Bridge provides a streamlined way to automatically synchronize data from Okta to SailPoint IdentityIQ, enabling an IAM capability for hybrid environments. With it, users, applications, accounts, and certification actions can be managed together. Because the solution is scalable, you can run one application or multiple in a single cycle. It is also modular, so you can automatically sync artifacts or selected components.

KPMG Cloud Identity Governance Bridge links IdentityIQ and Okta, delivering greater integration and stronger governance for cloud and on-premises applications. The bridge capability aggregates and imports applications in Okta as applications in IdentityIQ with the same fine-grained, attribute-level details present in Okta. Unlike the out-of-the-box connector that certifies Okta applications as entitlements, KPMG Cloud Identity Governance Bridge supports certification as applications so approvers see all fine-grained details during certification with different applications having different sets of entitlements. Lists of attributes for each onboarded application in IdentityIQ are driven by its definition in Okta.

KPMG Cloud Identity Governance Bridge enables IT departments to:

- Enable enterprises to leverage their current investment in SailPoint Identity IQ for digital identity lifecycle and governance activities
- Demonstrate compliance and fulfillment using closed-loop remediation from Identity IQ to Okta
- Rapidly onboard applications from Okta to IdentityIQ
- Save time and budget by reducing the manual effort needed to create SailPoint artifacts
- Reduce costs by reducing duplication of effort in both IAM tools
- Reduce manual configuration errors.

Easy to use, configure, and maintain, KPMG Cloud Identity Governance Bridge can help you manage, control, and secure cloud and on-premises applications in today's hybrid environments.

A robust capability that continues to improve
The current iteration of KPMG Cloud Identity Governance Bridge utilized by KPMG IAM professionals provides either scheduled or on-demand synchronization of users, applications, and user accounts from Okta to IdentityIQ. It also provides closed-loop remediation of certification actions from the bridge solution to Okta.

Future enhancements will soon offer user password synchronization, role and group synchronization, entitlement synchronization, and account synchronization from IdentityIQ to Okta.

Contact us

Jim Wilhelm
Principal, Cyber Security Services
T: 267-256-7271
E: jameswilhelm@kpmg.com

Debbie Patterson
Alliance Senior Director
T: 512-423-6150
E: deborahpatterson@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia