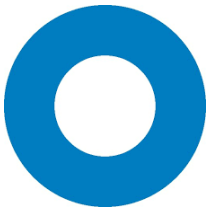


Okta and SailPoint Integration Guide (July 2018)

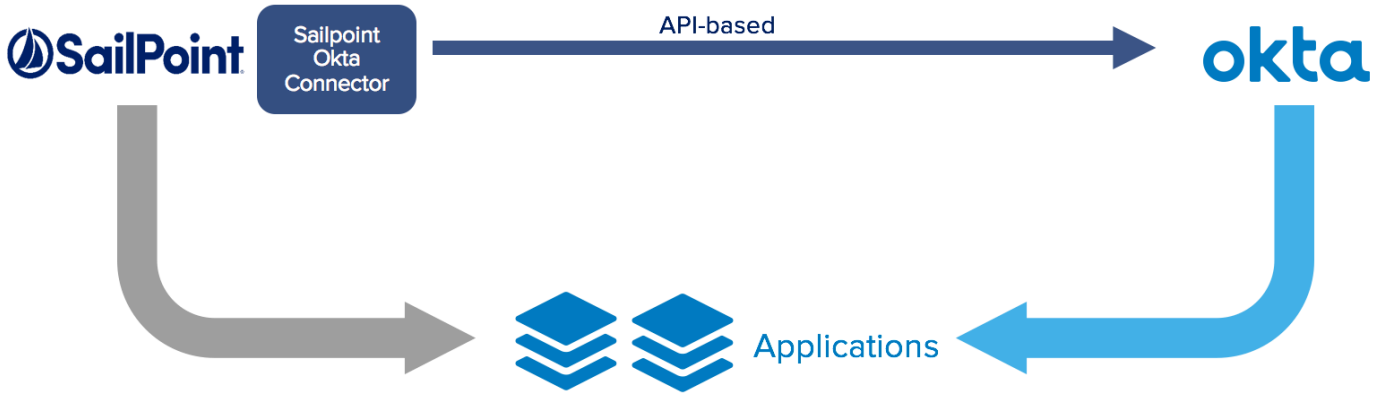
Table of Contents

Introduction

The partnership between Okta and SailPoint brings together two best-of-breed solutions to facilitate your Access Management and Identity Governance needs. This integration guide outlines best practices options by leveraging the Sailpoint-built Okta Connector or an Active Directory (AD) based integration pattern. Okta will be used as the main platform for User Authentication, Single Sign-On, Multifactor Authentication and Password Reset. SailPoint will be used as the main platform Access Request, Access Certification, Legacy Password Management and Compliance Controls. For Lifecycle Management and HR as a master, both Okta and Sailpoint can be used where it is appropriate.

Okta Connector

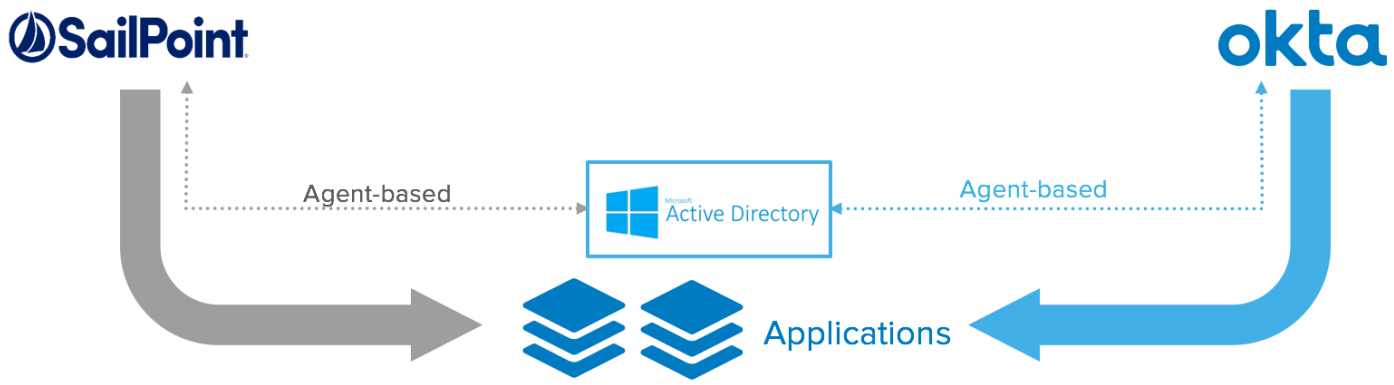
The Sailpoint-built Okta Connector uses Okta API for synchronizing user, group, entitlement and access information between the Okta and Sailpoint. The integration supports bi-directional use cases. For example, HR can be integrated with Okta – and information in Okta Universal Directory is aggregated by Sailpoint through the connector. Similarly, HR can be integrated with Sailpoint – and the information can be pushed to Okta through the connector.



Okta Connector using Okta API

Active Directory-based integration

In an Active Directory-based integration, both Okta and Sailpoint are connected to AD. All relevant users and their user profiles will be stored in AD - along with group information. AD will be used as the vehicle to relay changes about users, user profiles, groups and group memberships between Okta and SailPoint. This integration is also bi-directional regardless of whether Okta or Sailpoint is the source.



Active Directory based integration using agents

Integration with HRMS

User onboarding typically starts from a user's HRMS. Depending on the customer's existing deployment, the HRMS can be connected with SailPoint or with Okta depending on the types of HRMS. The HRMS will typically be the primary authoritative source of identity data for the integrated solution.

Integration with Active Directory

If AD is present, it is likely that both Okta and Sailpoint will be integrated with AD via their respective agents. As the Identity Provider, Okta treats AD as the authentication source where user passwords reside. At runtime, user credentials will be validated by Okta using the Okta Active Directory Agent.

As mentioned above, in an AD-based integration, the agents will be used to synchronize user, group and access information between the two systems.

Access Management

End users will authenticate into and access applications through Okta. Applications supporting single sign-on (SSO) protocols (SAML, OpenID Connect, etc.) will be integrated with Okta, and Okta will act as the Identity Provider. In addition, Okta Secure Web Authentication (SWA) provides a secure password vault for applications that do not support any federated SSO protocols.

In addition to SSO, MultiFactor Authentication (MFA) can be configured through Okta to further secure access during authentication into Okta and/or during application SSO.

Lifecycle Management

In a best-practice implementation, Lifecycle Management can be implemented in Okta and/or Sailpoint depending on the applications and systems. With the bi-directional nature of the integration between Okta and Sailpoint, both systems can relay the necessary user and group information to the other – regardless of which system the authoritiative source (eg. HRMS) is integrated with.

Access policies can be defined in both Okta and Sailpoint to drive provisioning across applications. For best practices, whenever additional compliance controls is needed for a target application, Sailpoint will handle the lifecycle management for that application. These compliance controls, such as Separation-of-Duty (SoD), can also be put in place and be enforced by Sailpoint during automated provisioning, account request, access certification or any other action triggered by other lifecycle changes. SoD is currently supported in IdentityIQ and is forethcoming in IdentityNow.

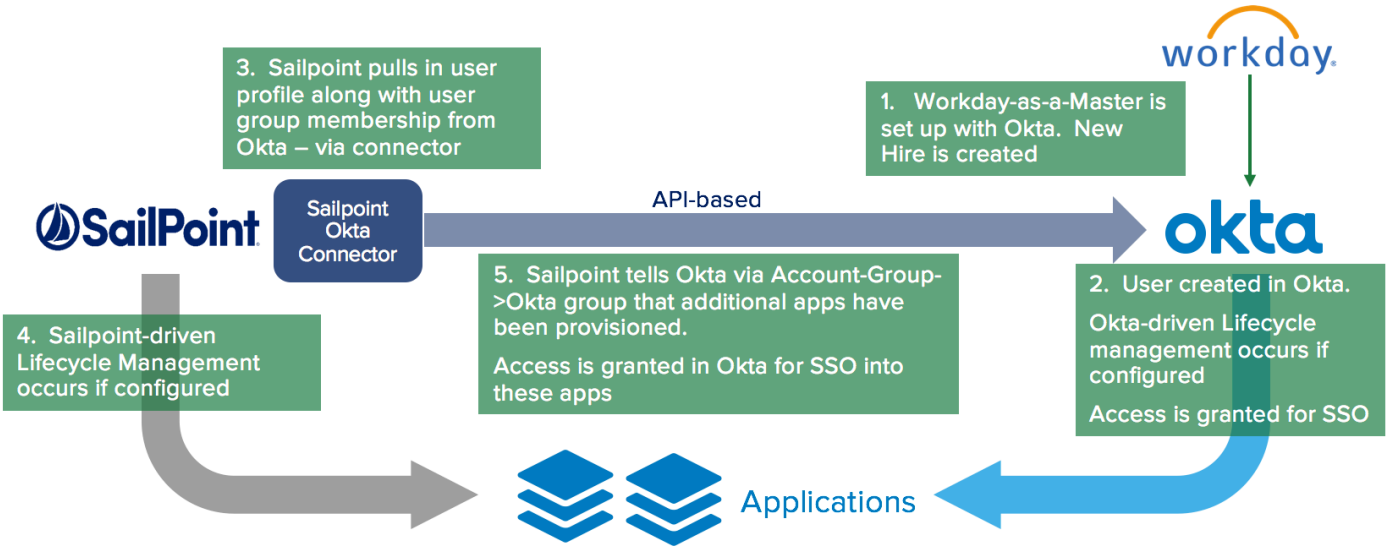
In Okta, an application assignment needs to occur in order for a user to SSO into any application. When Okta handles Lifecycle Management of an application, user is automatically assigned the application. When SailPoint handles Lifecycle Management of an application, Sailpoint will update Okta whenever a user is granted access to that application where SSO is needed.

For best practices, access policies in Okta and Sailpoint should be aligned to facilitate application assignments, access request and access certification. In particular, access entitlements and access profiles associated with the Okta source in Sailpoint should be aligned with Okta groups in Okta.

Connector-based integration example

In a connector-based integration, the Okta Connector relays information back and forth between Okta and Sailpoint. The following example assumes Workday-as-a-master implemented with Okta which is where the user lifecycle begins. The Okta Connector can aggregate information from Okta Universal Directory via Okta API when information needs to flow from Okta to Sailpoint. When changes in Sailpoint need to be reflected in Okta, the Okta Connector pushes that information to Okta via Okta API.

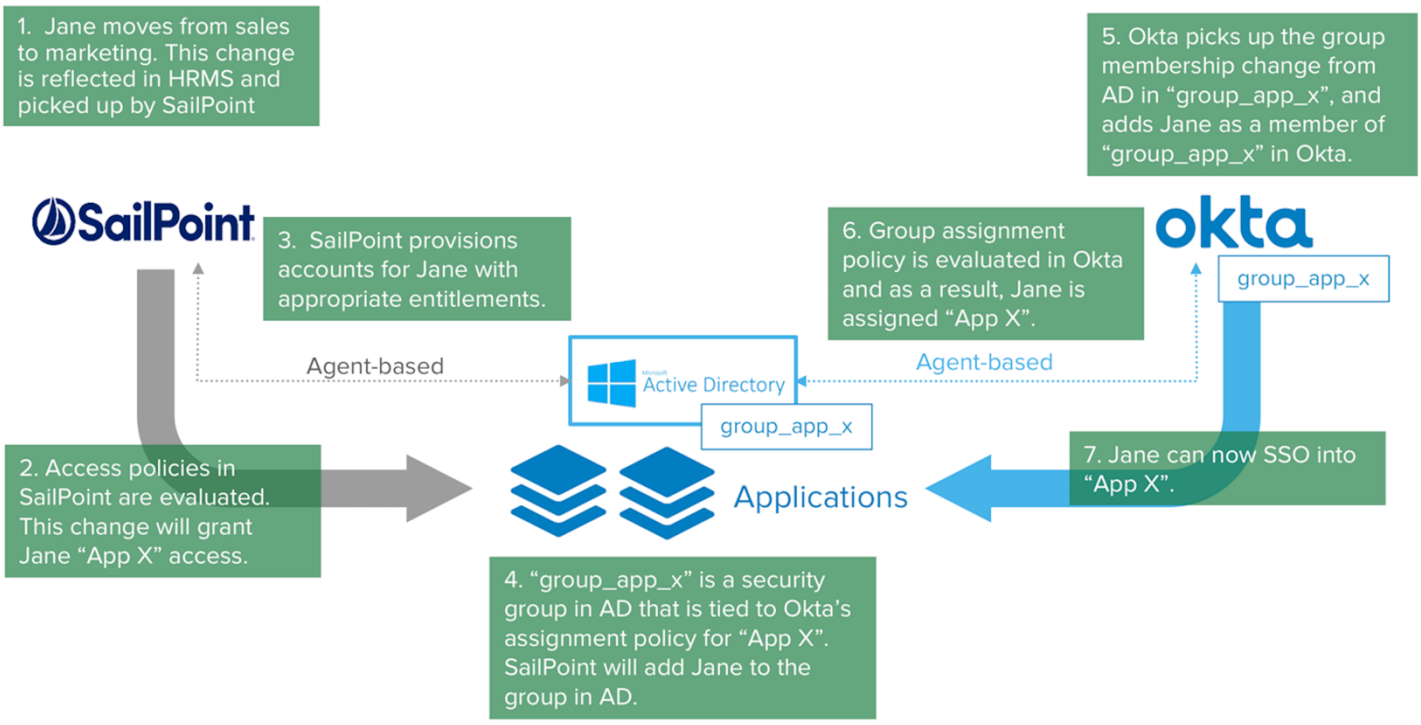
The following diagram illustrates a sample “on-boarding” flow.



AD-based integration example

In an AD-based integration, AD is used as the bridge to propagate the users' group assignment; SailPoint provisions the group on AD, and then Okta reads the AD group setting and makes its assigments automatically.

The following diagram illustrates a sample "mover" flow using AD as a bridge.



Access Request

Access Request, as part of lifecycle management, will be handled by SailPoint. Similar to the lifecycle management scenario above - Okta groups can be used to propagate the result of an access request from SailPoint to Okta for the purposes of application assignment. Depending on whether lifecycle management is handled by Okta for a particular application, an application assignment may result in Okta provisioning an account in addition to providing SSO for that application. In SailPoint, the groups that provide application access should be associated with a requestable application (in IdentityNow), or included in a "requestable" role (in IdentityIQ). Once the request and approval workflow has completed, SailPoint will trigger the necessary user/group changes in Okta to complete the request.

Access Certification

SailPoint handles access certification with out-of-the-box support to certify applications, users and groups. To initiate compliance activities on an Okta application, where access is controlled by membership to a group assignment either on Active Directory or directly within Okta, you can build certification campaigns around applications, users and groups as follows:

1. Certify the Active Directory or Okta source
2. Certify the User assigned to the Group
3. Certify the Group Membership

During certification, if a decision is made to revoke user access as part of remediation, the actual deprovisioning can occur automatically and immediately. For applications where lifecycle management is done in Sailpoint, SailPoint will handle the actual act of deprovisioning or disabling an account. If Okta is managing the application, similar to Access Request, Sailpoint can alert Okta of the change via the Okta Connector through an Okta group which will then allow Okta to deprovision access accordingly.

Password Reset

Since the authentication experience and SSO is done in Okta, Password Reset will be initiated through Okta. Assuming AD is in place as the authentication source, the initial password change will happen in AD via Okta Active Directory Agent. This change can be picked up by SailPoint via the Password Interceptor tool which is included with every SailPoint deployment. SailPoint can then be configured to react to this password change, allowing for the change to be synchronized across additional connected systems.

Support for Okta Connector-based password reset is on the roadmap.

Single Sign-On into SailPoint

For better user experience, SailPoint will be configured as a service provider to Okta so that end users needing to access SailPoint can SSO from Okta.