okta

Custom App Integration

Okta Inc.
301 Brannan Street
San Francisco, CA 94107

Introduction

Enterprises and large public institutions have deeply integrated application architectures with legacy IAM systems. They have a gamut of vendors, products, solutions, gateways and components that service legacy architectures and use cases. As use cases need to change, it's very hard to change the underlying stack. There is too much built-in logic and solution engineering. They are challenged with the need for greater agility and introducing the right architecture for the future while managing the transition of the legacy architectural approaches.

Legacy packaged software required heavy customization to deploy. Then, it would require a massive amount of re-engineering to do upgrades or maintenance. The world is moving to cloud platforms that are always up to date, never requiring forklift upgrades. These cloud platforms have considerable out-of-the box capabilities. However, the need for customization does not just go away. Cloud platforms need to integrate with every system in the enterprise, including packaged on-prem software as well as fully custom applications.

Okta Identity Cloud – Always On Foundation for IAM Integration

Okta is the leading IDaaS (i.e. IAM cloud service) today, and is delivered entirely as a multi-tenant cloud service. All Okta capability across Access Management (e.g. SSO, MFA, adaptive authentication, API security) and Lifecycle Management (e.g. provisioning, lifecycle orchestration, governance reporting) is delivered out of the box as a cloud service. Okta maintains the service on the customer's behalf, delivering extremely high reliability and uptime as well as maintaining world-class security of the service (e.g. 3rd party PEN tested, SOC 2 Type II and the only IDaaS with CSA Star Level 2 Attestation).

The Okta Identity Cloud comes pre-integrated to 5000+ applications out-of-the-box. However, to use Okta as an enterprise-wide IAM platform, large enterprise and public sector customers require integration to a multitude of on-prem and custom applications. Okta provides several mechanisms across products to enable integration to these systems.

Access Management Custom Integration

For Access Management, Okta has invested in product capabilities around federation that represent the future direction of the market. However, to fully support the modern hybrid enterprise IT environment, customers can follow a number of approaches for integrating all of their applications to Okta.

The methods Okta uses for custom integration to applications depends on the type of application. The following are some examples.

Modern Custom Applications

Any application that supports federation can be directly integrated to Okta. Custom integrations can be configured in Okta for SAML, WS-FED or OpenID Connect (OIDC). OIDC is particularly popular among developers today, since it is the most modern federation standard and it is easier to implement in the application than older federation standards.

Custom Applications that Can Be SAML-enabled

Many applications that support a standard reverse proxy architecture that run on modern web application platforms, such as Microsoft IIS, IBM WebSphere, Oracle WebLogic and Apache JBOSS can be modernized to support federation. These web servers all provide containers that can be SAML-enabled (or WS-Fed enabled). Okta would then directly integrate to all of these applications via SAML. Alternatively, some applications can be SAML-enabled by directly modifying the authN package on the app.

Okta provides SAML toolkits to assist with SAML-enabling applications. In addition, if a customer needs assistance in configuring these applications, Okta offers professional services to assist with this work. Okta provides guidance for retrofitting or upgrading applications to support federation. Many customers will have Okta help configure a few applications, then do the rest of them themselves.

Applications that Can Not be Enabled for Federation

For applications that do not support federation, and use HTTP headers for single sign-on or other protocols that require an on-prem STS, such as Exchange NTLM or Kerberos, Okta has taken an approach of partnering with network gateway vendors to offer a complete solution.

Agent-based approaches for header-based access management have been challenging for enterprises to deploy. However, proxy-based approaches are really something better served by a best-of-breed network gateway. Such products were built to handle large loads of network traffic and proxying and modifying the traffic along the way. Modifying HTTP headers is an aspect of the core capability of these products.

Okta partners closely with leading networking vendors such as F5, Citrix and Palo Alto Networks so that customers that have already invested in those gateways can seamlessly use their existing investments with Okta. Okta has invested in comprehensive integration guides and added them as "applications" in the Okta Application Network (OAN) to make these integrations easy to deploy. For greenfield customers, we have partnered with Akamai Enterprise Application Access (formerly SOHA) as a lightweight gateway and have a system integration partner, ICSynergy, that can deploy open source technology with customization.

In all scenarios, Okta remains the central point of authentication and authorization for access to the end resource, and provides the authoritative attributes about the user via SAML to the gateway or to the app server.

Packaged Software

Integration to commercial packaged software often depends on the specific platform involved.

- Oracle Enterprise Business Suite – Newer versions often support SAML directly. For older versions, Okta Professional Services would handle this on a case-by-case basis. In some cases an Okta system integration parter may be involved, or, integration to Oracle Access Manager may be required.
- SAP – Uses a proprietary reverse proxy architecture. Generally, SAP environments are fronted by Netweaver, and Netweaver 7.4 or 7.6 support SAML natively. Okta would integrate to Netweaver via SAML.

- Citrix - NetScaler is in the Okta Application Network, and Okta provides a supplemental comprehensive integration guide to NetScaler, XenApp and XenDesktop. Generally, this involves a SAML integration to NetScaler with specific configuration of Okta and NetScaler to support XenApp and XenDesktop or other web apps protected by NetScaler.
- SharePoint Server - Would integrate via WS-Fed. If users need to access embedded SharePoint applications that are protected, such as BI features, Okta would configure the Windows Identity Foundation claims to Windows token service (WIF c2WTS) for translation from WS-Fed to Kerberos.

Mobile Apps that Make Calls to APIs

Okta API Access Management would be used to secure access to the API for access by the mobile app, in the context of the user's access permissions.

Applications that Do Not Support Proxy or Agent Technology, or Federation

Password vaulting, forwarding and form-filling, called Okta Secure Web Authentication (SWA) is the method of last resort Okta can use that covers any application with a login form. Okta does this through a browser plug-in/extension. Our capabilities here are unique:

- Uses a heuristic to automatically configure sign-in at the moment the user goes to access the application. This provides for automatic configuration of SSO to any login form, and it ensures that SSO will continue to work if a login form changes
- Can be configured to use any form of username, and have the username preconfigured by an admin
- Can be configured to use the same password as a user's AD/LDAP or Okta password. If the app does not already have a synced version of AD credentials, or does not authenticate against AD, Okta Lifecycle Management can often be used to sync the user's password to the app as well. This complete solution of syncing the password and then forwarding the user's AD/LDAP/Okta password to the app for authentication provides a "federation-like" experience to the end-user that requires zero password management by the end-user
- Several other password management options, including sharing credentials among users and varying amounts of admin control vs. user configuration

Lifecycle Management Custom Integration

For provisioning and lifecycle management integration to applications, Okta comes with 80+ applications pre-integrated for provisioning. To extend provisioning to any applications, Okta includes the following methods:

On-prem Provisioning Agent and SDK

Okta provides an on-prem agent that extends the Okta provisioning capability behind a customer’s firewall with zero firewall changes, and has built-in high availability. The agent has a SCIM interface that enables direct integration with any application supporting SCIM, and includes an SDK that enables customers to write a connector to integrate any application. Okta Professional Services has experience integrating SAP and Oracle to Okta via the on-prem provisioning agent. This includes outbound provisioning as well as mastering from applications, such as HRIS.

Public SaaS App with No Existing Provisioning Support in Okta Application Network (OAN)

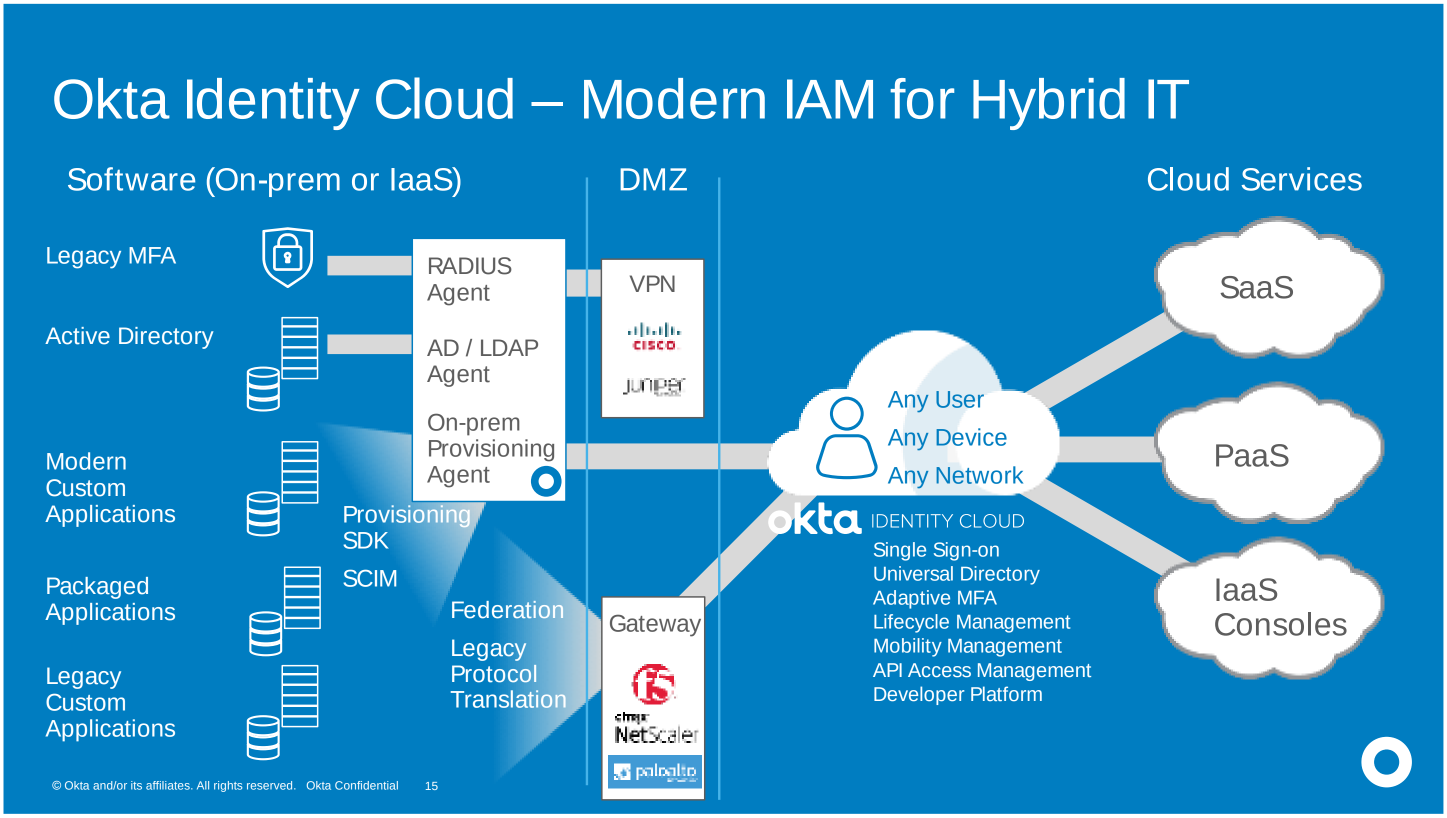
Many ISVs are now taking the initiative on their own to integrate their applications to Okta for provisioning and lifecycle management using SCIM. Okta provides dev tools, training, QA and support, and verifies the integration before publishing it in the OAN. Using the SCIM app template, Okta provides a full set of documentation and guidance that a developer can follow on his own to SCIM-enable an application (see http://developer.okta.com/standards/SCIM/). There are numerous resources available that will allow a developer to start from a foundational code-base that they can then modify for their specific application. For example, SCIM Server templates can be found on GitHub. Once approved, Okta makes the integration available to all customers. There are already over 100 ISVs registered in the program and a host of ISV-built published integrations, including Envoy, Github, Lucidchart and more. ISVs interested in more details can go to http://developer.okta.com/standards/SCIM/ or email developers@okta.com.

Okta API

The Okta API provides a REST interface that can be used to create, read, update and delete users from any script or code written, from anywhere, behind the firewall or in the cloud. Okta professional services has extensive experience with connecting any application for provisioning via the Okta API.

Summary

The Okta Identity Cloud is a secure, highly available service that provides broad IAM capabilities out-of-the-box. Okta has 40+ feature releases a year, and ever customer on Okta is always on the same codebase. There are never any patches or forklift upgrades. Okta handles this transparently with a zero downtime architecture that is never taken offline for updates or maintenance.



Okta Identity Cloud – Modern IAM for Hybrid IT

Software (On-prem or IaaS)

DMZ

Cloud Services

Legacy MFA

Active Directory

Modern Custom Applications

Packaged Applications

Legacy Custom Applications

RADIUS Agent

AD / LDAP Agent

On-prem Provisioning Agent

Provisioning SDK

SCIM

Federation

Legacy Protocol Translation

VPN

Gateway

Any User

Any Device

Any Network

okta IDENTITY CLOUD

Single Sign-on

Universal Directory

Adaptive MFA

Lifecycle Management

Mobility Management

API Access Management

Developer Platform

SaaS

PaaS

IaaS Consoles

Over 5000+ applications come pre-integrated to Okta, however enterprises and public sector organizations require Okta to integrate to every application, including custom applications and packaged software. Okta provides several custom integration methods across Access Management and Lifecycle Management to enable Okta to extend to support IAM across a broad hybrid IT environment.