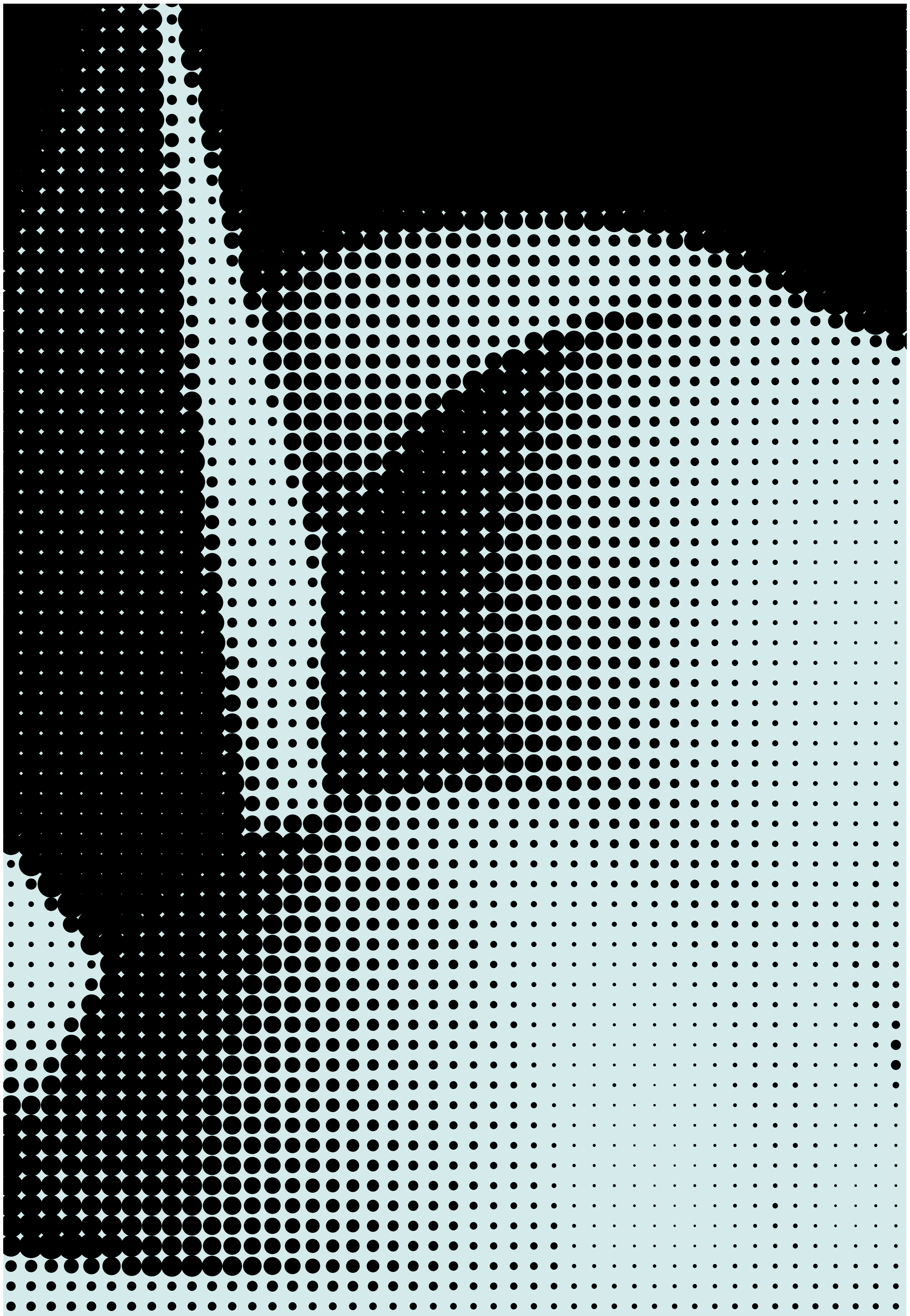
Whitepaper

November 2020

How Okta Integrates Applications

An architectural overview

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871



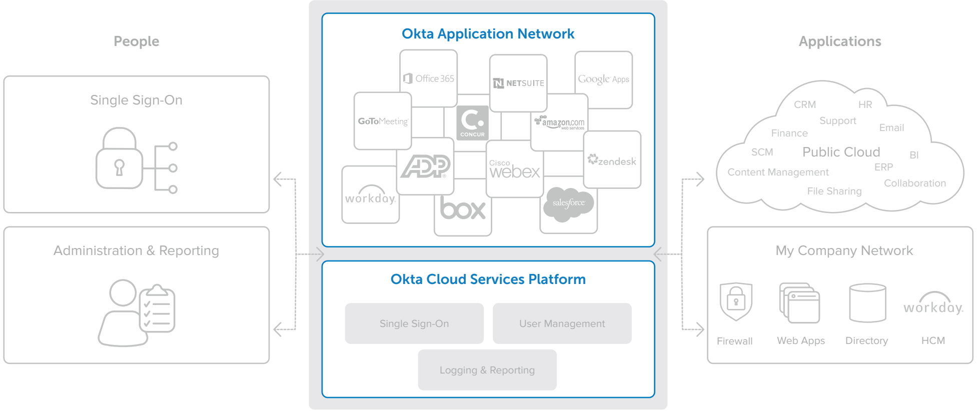
Contents

Okta: Enterprise Identity, Delivered

Okta is an enterprise grade identity management service, built from the ground up in the cloud and delivered with an unwavering focus on customer success. With Okta IT can manage access across any application, person or device. Whether the people are employees, partners or customers or the applications are in the cloud, on premises or on a mobile device, Okta helps IT become more secure, make people more productive, and maintain compliance.

Integrating Applications with the Okta Service

Unlike other identity management solutions, Okta is not simply a toolkit that you use to connect your web applications to your user directories. That takes too much of your time and resources. Instead, Okta "integrates" applications into its service for you, and you simply deploy these pre-integrated applications to your users as necessary. You can authenticate these users against your own user store (e.g. Active Directory or LDAP) or you can use Okta as the user store. Okta is unique in providing quick, feature rich integrations with web based and native mobile applications, whether these are in the cloud, on-premises or on your smartphone or tablet. These integrations are delivered as a part of the Okta service and include both SSO and user management capabilities. This document describes the various ways Okta integrates applications into its service.



Okta: Managing Access across Any Application, Device or Person

Cloud, On-premises, and Mobile Applications

It is useful to start with a distinction between cloud, on-premises and mobile apps.

For typical cloud based applications (e.g. Salesforce, Google Apps, Workday, etc.), these integrations are delivered as a part of Okta's Application Network. Administrators simply select from Okta's list of thousands of supported applications, use a simple wizard answering basic questions about their specific instance of the applications (such as URL and administrative IDs) and Okta handles the rest.

All technical details (such as SSO protocols and user management API implementations) are encapsulated in the service and continually maintained by Okta on your behalf. These applications may use a standard like SAML or OpenID, they may use a proprietary API, or they may use Okta's Secure Web Authentication (SWA) protocol.

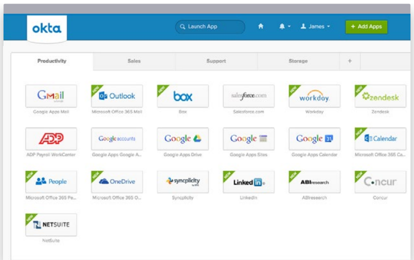
Many of the most popular on premises web based applications (Oracle Apps, Lawson, Jira, etc.) are also included in the Okta Application Network. For custom developed on-premises web based applications Okta provides a range of integration options as well. Secure Web Authentication integration for SSO can be easily added, Okta has SAML toolkits that can be used to SAML enable your apps, and Okta also supports provisioning and deprovisioning into applications that expose user management APIs publicly.

Okta also provides easy access to mobile enterprise applications from any device. Whether your enterprise apps are HTML5 web apps optimized for mobile platforms or Native iOS or Android apps, Okta has a solution. Any web application in the Okta Application Network can be accessed with single sign on from any mobile device. Mobile web apps can use industry standard SAML, or they can use Okta's Secure Web Authentication SSO technology. Native applications like Box Mobile can be integrated using SAML authentication for registration and OAuth for ongoing use.

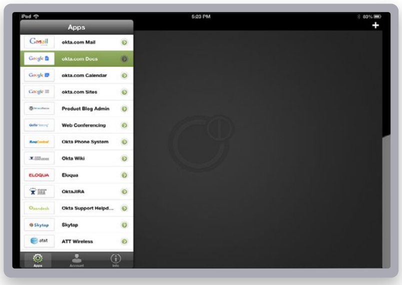
Single Sign-On to ANY Application

Okta creates a seamless user experience by providing single sign-on to ALL of the web and mobile applications users need. Users log in once, and can then launch each application without having to re-enter credentials. It is important to note that this SSO experience only works well when ALL applications are covered; if some applications cannot be supported then it's not truly single sign-on. For this reason, Okta employs several methods to enable SSO into different web applications.

Okta first establishes a securely authenticated session with the user's browser. Once this session has been established, Okta can authenticate the user to any connected application using one of two SSO integration methods. Okta's SSO integrations can either be federated (i.e. supporting a standard such as SAML or another proprietary federated authentication protocol) or they can leverage Okta's Secure Web Authentication (SWA) to perform a secure, form-driven post to the application login page, signing in the user automatically on their behalf.



Okta's "My Applications" landing page provides a simple launch point to all applications.



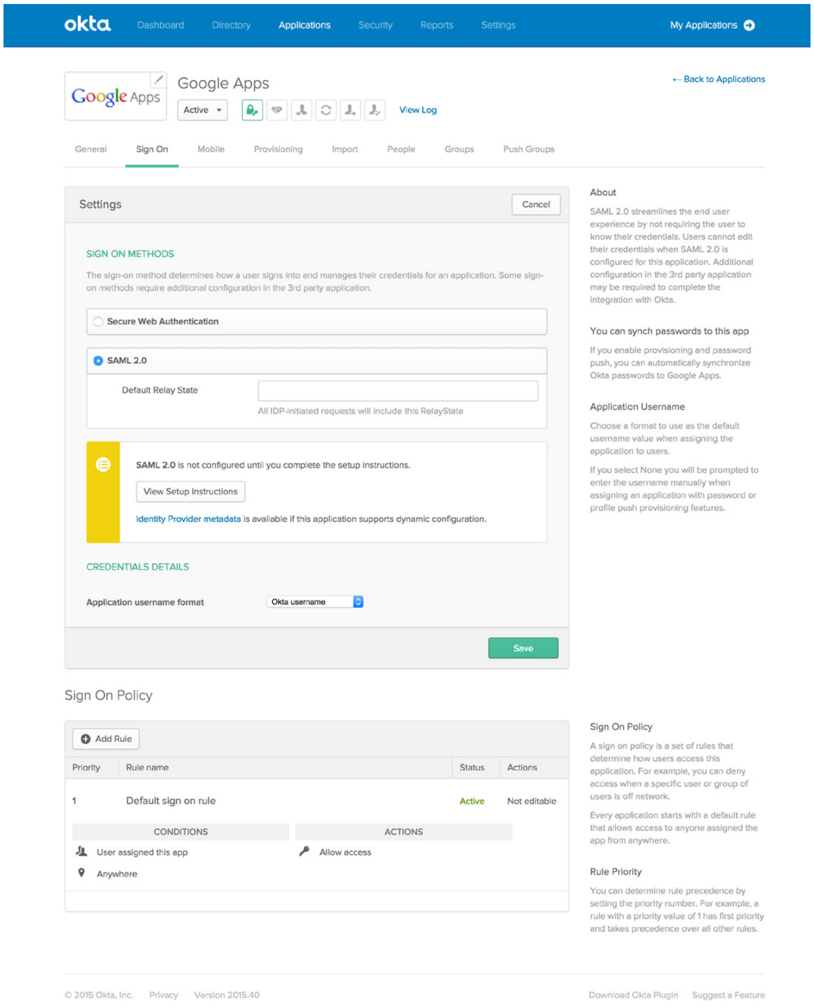
Okta's Native iOS app runs on iPADs and iPhones.

Standards based SSO

There are multiple Standards-based ways to do SSO. Because Okta is a cloud service, we have the ability to add support for any standards, i.e. we are not forced to choose one standard or another.

Okta supports numerous federated SSO protocols including standards such as SAML (1.1 and 2.0). Some application vendors only support proprietary federated SSO protocols, but Okta supports those as well so that you don't have to worry—it just works. If an application needs authorization support for OpenID, Okta can easily add support for that application too.

Every time Okta adds a new application to its network, every one of our customers immediately gets access to that application; this is why Okta can spend its engineering resources to support all authentication standards.



Google Apps

Settings

SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

○ Secure Web Authentication

● SAML 2.0

Default Relay State

All IDP-initiated requests will include this RelayState

SAML 2.0 is not configured until you complete the setup instructions.

Identity Provider metadata is available if this application supports dynamic configuration.

CREDENTIALS DETAILS

Application username format: Okta username

About

SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

You can synch passwords to this app

If you enable provisioning and password push, you can automatically synchronize Okta passwords to Google Apps.

Application Username

Choose a format to use as the default username value when assigning the application to users.

If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

Sign On Policy

Priority	Rule name	Status	Actions
1	Default sign on rule	Active	Not editable

CONDITIONS	ACTIONS
User assigned this app	Allow access
Anywhere	

Sign On Policy

A sign on policy is a set of rules that determine how users access this application. For example, you can deny access when a specific user or group of users is off network.

Every application starts with a default rule that allows access to anyone assigned the app from anywhere.

Rule Priority

You can determine rule precedence by setting the priority number. For example, a rule with a priority value of 1 has first priority and takes precedence over all other rules.

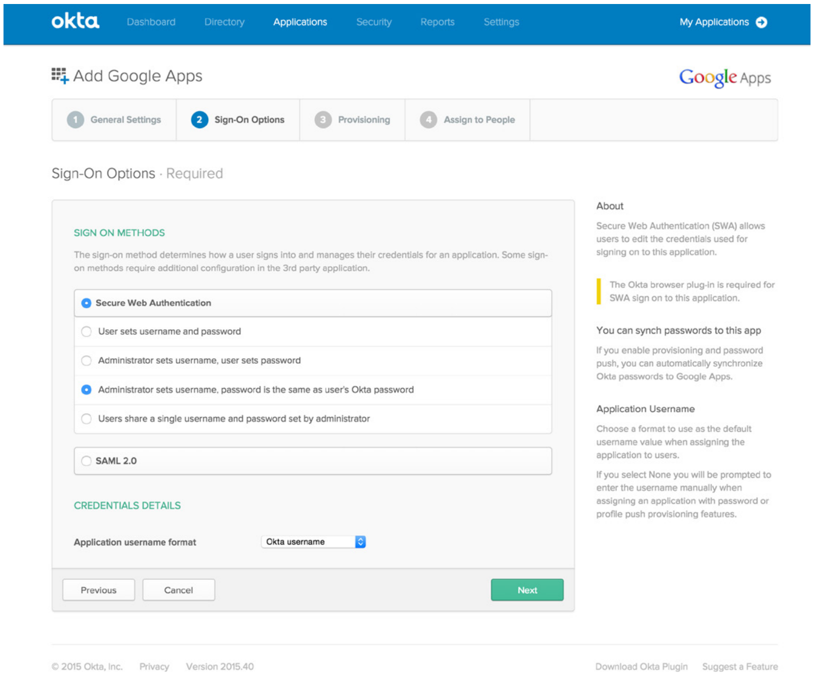
Configuring Google Apps for SAML 2.0 SSO

Secure Web Authentication (SWA) for SSO

For web applications that do not provide support for federated single sign-on Okta has developed our Secure Web Authentication (SWA) technology.

When SWA is enabled on an application, end users see an additional link below the application icon on their Okta home page, and through this link users can set and update their credential in the secure store for that application only. The credential is stored in an encrypted format using strong AES encryption combined with a customer specific private key. When a user subsequently clicks the application icon, Okta securely posts the username/password to the app login page over SSL and the user is automatically logged in.

SWA can optionally be made even easier for end users; admins can require the username and password that is used for SWA-based apps to be the same as that user's Okta credentials, removing one more step for end users (they are no longer prompted for the initial password entry).



Sign-On Options · Required

SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

- ● Secure Web Authentication
  - ○ User sets username and password
  - ○ Administrator sets username, user sets password
  - ● Administrator sets username, password is the same as user's Okta password
  - ○ Users share a single username and password set by administrator
- ○ SAML 2.0

CREDENTIALS DETAILS

Application username format: Okta username

About

Secure Web Authentication (SWA) allows users to edit the credentials used for signing on to this application.

The Okta browser plug-in is required for SWA sign on to this application.

You can synch passwords to this app

If you enable provisioning and password push, you can automatically synchronize Okta passwords to Google Apps.

Application Username

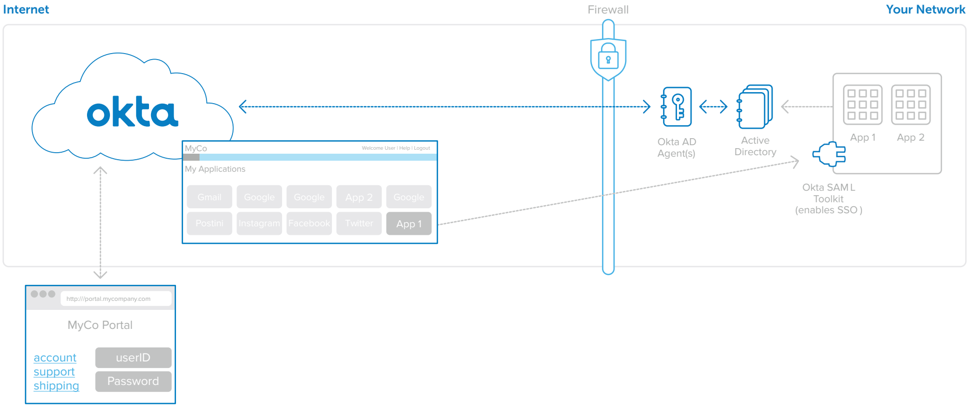
Choose a format to use as the default username value when assigning the application to users.

If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

Configuring Google Apps for SWA–based SSO

SAML Toolkits for SSO

For custom web applications that are not in the Okta Application Network, Okta also provides integration toolkits to easily enable these applications to support SAML. The SAML integration toolkits are available for .NET, Java and PHP platforms.



Using Okta's SAML Toolkit to enable SSO for on-premises web applications

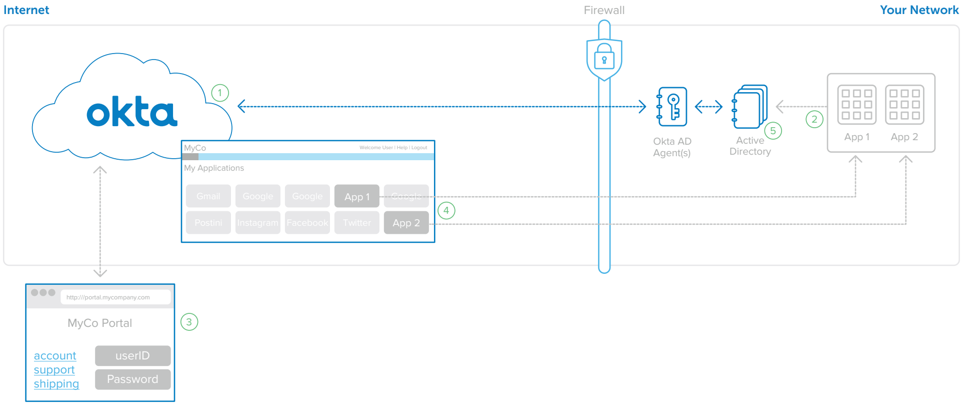
Single Sign-On for Active Directory Authenticated Web Apps

Most enterprises have on-premises web applications that can easily be integrated into Okta's SSO solution. Many companies also have on-prem web applications that use Active Directory credentials for authentication. These applications are not using Integrated Windows Authentication, but instead require the user to enter their AD credentials when they sign in via a browser. When Okta is configured to delegate authentication to Active Directory, signing in to these internal web applications can also be automated.

The behind-the-scenes steps that enable SSO for AD authenticated internal web applications (shown below) are:

1. Okta is configured to delegate authentication to AD.
2. Customer has on-premises apps authenticating to AD.
3. User logs into Okta with AD credentials.
4. User accesses App 1 and App 2 with SWA using AD credentials.
5. App 1 and App 2 authenticate user against AD.

Okta can leverage its Secure Web Authentication protocol to automatically log users into these internal web applications. When an internal web application is configured to delegate authentication to AD (the same source to which Okta delegates authentication), Okta captures the user's AD password at login and automatically sets that password for that user in any applications that also delegate to AD. This allows users to simply click a link to access these applications, and then be logged in automatically. Note that Okta synchronizes the AD password securely; if the password subsequently changes in AD, this event is captured on login to Okta and immediately updated in the secure password store for that application, ensuring that the next login attempt will be successful.



Okta enables SSO for AD authenticated internal web applications

Enabling User Management

User management is defined as the provisioning of new accounts for new users, deprovisioning of accounts for deactivated users, and keeping user attributes synchronized across multiple directories as necessary. Okta's user management features enable the service to automatically manage user accounts within applications, saving you time and money and ensuring correct access privileges are always up to date. User management is bidirectional, so accounts can be created inside the application and imported into Okta, or account information can be added to Okta and then pushed to the corresponding applications.

There are three core areas of user management functionality that Okta provides:

1. Bulk user import (from a variety of sources)
2. Ability to natively create, read, update, and delete (CRUD) users within Okta
3. Password synchronization / password push (across multiple directories)

For user management integrations Okta supports OAuth 2.0 based authentication, and if an application supports lesser known standards such as SCIM or SPML, Okta can leverage those for user management as well. Similar to SSO access, Okta does the work of connecting to these APIs for you; there is no "connector" work for you to do yourself. To enable user management you simply configure Okta with credentials for your API user and select the features that you would like. Everything else is handled by the Okta service, including continuous automated testing and (if necessary) updates as the capabilities of the application inevitably evolve.

On-premises applications can also be integrated into Okta to enable user management. This can be done in one of two ways: leveraging Active Directory or using web services to manage user accounts in applications:

- For enterprises that on-board users via an HRMS like Workday, Okta can support user management into on-premises applications by using Active Directory as a meeting point. You can configure Okta to mange accounts in your Active Directory instance, and Okta will create and update users in AD based on user accounts in Workday. This information can then be used by any on-premises web application that uses Active Directory as its user store.

- Alternatively, Okta's can support user management for any on-premises web application that has a web services API that can be made available to the Okta service via a publicly addressable connection. Okta will make calls to that application's web service to create new user accounts, update attributes, and deactivate users as needed based on the user assignment rules configured in the Okta service. Okta can provide detailed examples of web services APIs as well.

Conclusion

Single-sign on and user management are key requirements of any enterprise adopting cloud and mobile applications alongside their existing web-based on-prem applications. SSO, as the name implies, only truly works when all applications are covered, and therefore any credible SSO solution must support a variety of methods to integrate all the web and mobile applications you need to run your company. Okta uniquely enables SSO into any web or mobile application using open standards, or proprietary APIs, or Secure Web Authentication (SWA) and by SAML-enabling on-prem web applications. Additionally, user management comes pre-integrated for all of the cloud applications that support this functionality, and on premises apps can be easily incorporated via AD integration or by provisioning and de-provisioning directly to supported APIs.

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,500 application integrations, Okta customers can easily and securely use the best technologies for their business. To learn more, visit **okta.com**.