# Integration Patterns for Legacy Applications

okta

# Index


| | |
|---|---|
| Why should I integrate my apps with Okta? | 3 |
| Scope | 5 |
| When to use this eBook | 6 |
| How to read this eBook | 7 |
| **Integration patterns supported by Okta** | 8 |
| RADIUS | 9 |
| LDAP Cloud Interface | 11 |
| LDAP and Active Directory Synchronization | 13 |
| Security Assertion Markup Language (SAML) | 16 |
| Web Services Federation (WS-Federation) | 20 |
| OAuth | 22 |
| OpenID Connect (OIDC) | 25 |
| Reverse Proxies (Header-Based authentication) | 29 |
| Secure Web Authentication (SWA) | 31 |
| System for Cross-domain Identity Management (SCIM) | 33 |
| On-Premises Provisioning (OPP) | 35 |
| Time-Based One-Time Password (OATH-TOTP) | 37 |
| On-Premises MFA | 39 |
| Smart Cards and Personal Identity Verification cards (PIV) | 41 |
| FIDO U2F | 43 |
| Remote Desktop Protocol (RDP) | 45 |
| Secure Shell (SSH) | 49 |
| Okta Management APIs (REST APIs) | 52 |

# Why should I integrate my apps with Okta?

Okta Identity Cloud Service is an Identity as a Service (IDaaS) platform that helps you securely connect people to technology. The platform is cloud-native— 100% born and built in the cloud – and provides the following services:

**Single Sign-On (SSO)**

Allows your users to access multiple apps with a single authentication.

**Adaptive Multi-Factor Authentication (Adaptive MFA)**

Secures your Applications and your infrastructure – i.e., network appliances, VPNs, servers, and legacy IAM solutions – with a comprehensive set of modern verification factors and adaptive risk-based authentication.

**API Authorization (API-AM)**

Protects access to to APIs and custom apps using authentication and authorization protocols such as OpenID Connect and OAuth.

**User and Group Storage (Universal Directory)**

Stores your user and group data in a highly available solution and make them available for consumption by your apps in different protocols. Supports data customization and can consolidate any attributes across various identity sources.

**User and Group data synchronization with external systems (Lifecycle Management)**

Automates the user and group data management across multiple systems. Regularly pulls data from and push data to systems following your business rules and policies. Okta integrates with 100+ data stores including Active Directory, LDAP, HR systems such as Workday and

This eBook presents the patterns you can use to integrate your legacy or proprietary systems with Okta. These patterns are used daily by our customers to take maximum advantage of the Okta Identity Cloud Platform beyond the 6000+ integrations supported natively by Okta.

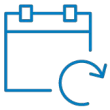
## Integrating your legacy or proprietary systems with Okta provides multiple benefits including:

Improve the security posture by implementing MFA and a tight account management

Improve the user experience when accessing your apps

Reduce operational costs and tasks related to user and infrastructure management

Improve resiliency by using a service that is globally available, has zero planned downtime – the service never shuts down for maintenance, and is regularly updated with security enhancements and new features.



Improve cost flexibility by using a subscription-based service.

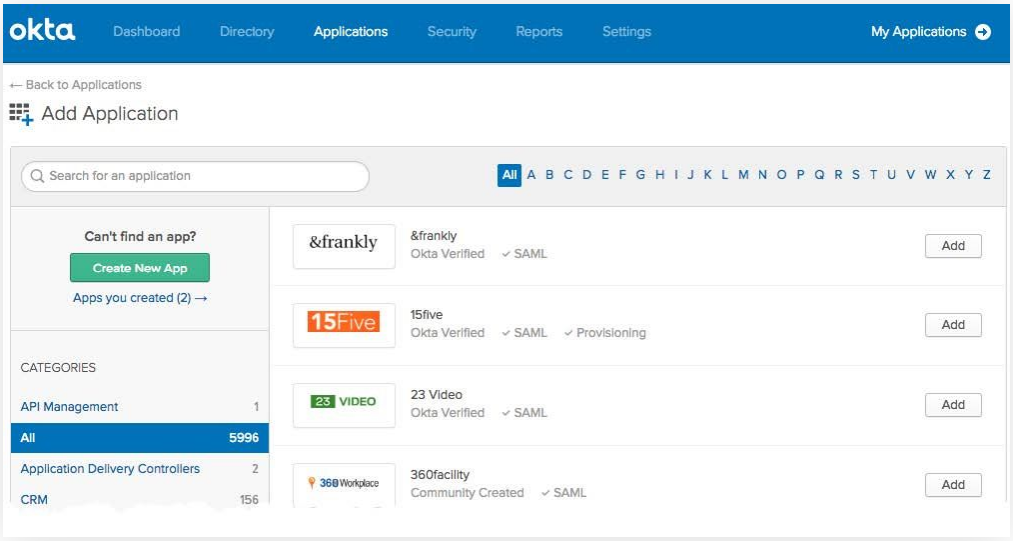
# Scope

## This guide covers:

- An architectural overview of the integration patterns supported by Okta
- A list of use cases and systems typically associated with each integration pattern
- Conceptual diagrams describing the major components in each integration pattern
- A list of documentation references for each pattern

## This guide doesn't cover:

- Native Integrations supported by Okta: Okta supports 6000+ integrations with 3rd party systems exposed in the Okta Integration Network catalog:

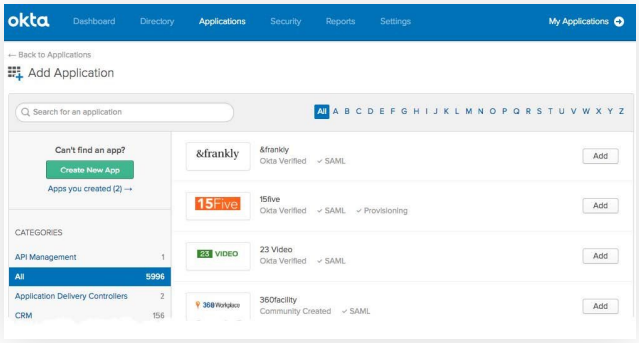



- Step-by-step procedures on how to integrate your legacy/proprietary systems with Okta.

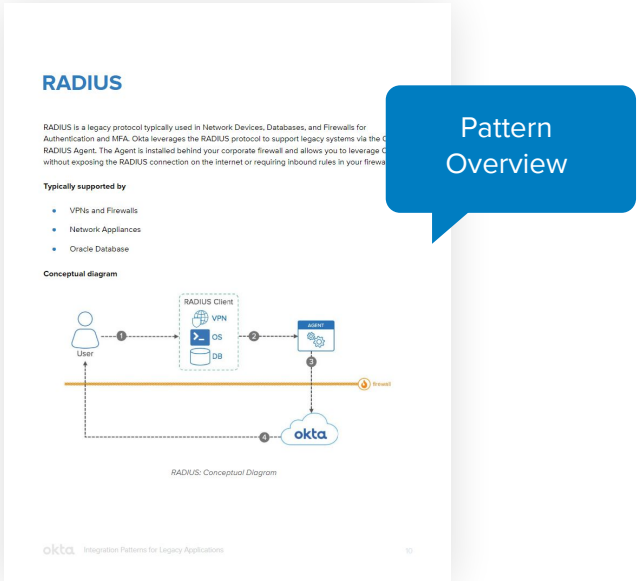
# When to use this eBook

The integration patterns can be used when you want to integrate a system with Okta that's not supported natively in the Okta Integration Network. To identify whether Okta supports your application:

1. **Confirm that your application is not listed in OIN**

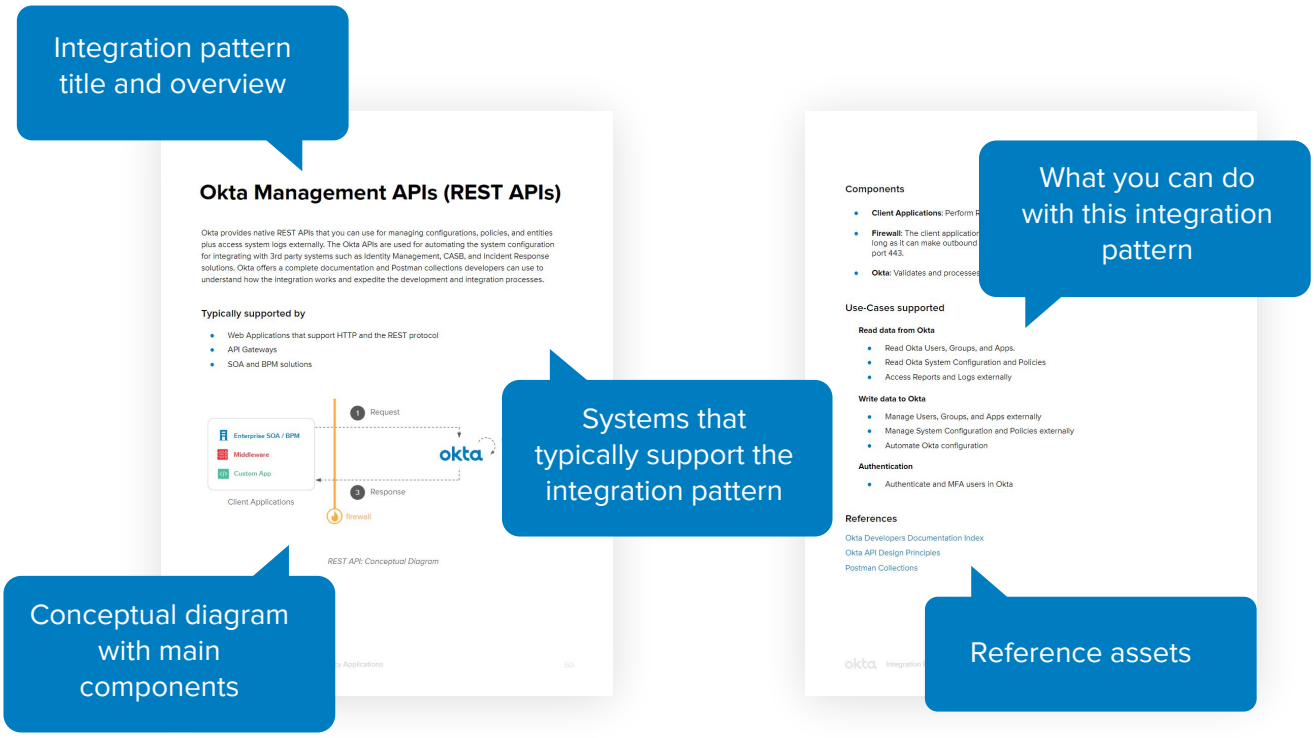



2. **Select and use the integration pattern based on your use-case and application**



# How to read this eBook

Each integration pattern is presented in its chapter:




*Integration Pattern supported by Okta: One chapter per integration.*

## Within each chapter, you find:

- An overview of the integration pattern
- What systems typically support the integration pattern
- A conceptual diagram describing the major components in the integration
- Use cases you can accomplish by implementing the integration
- A list of references you can use to further explore the integration

# Integration patterns supported by Okta

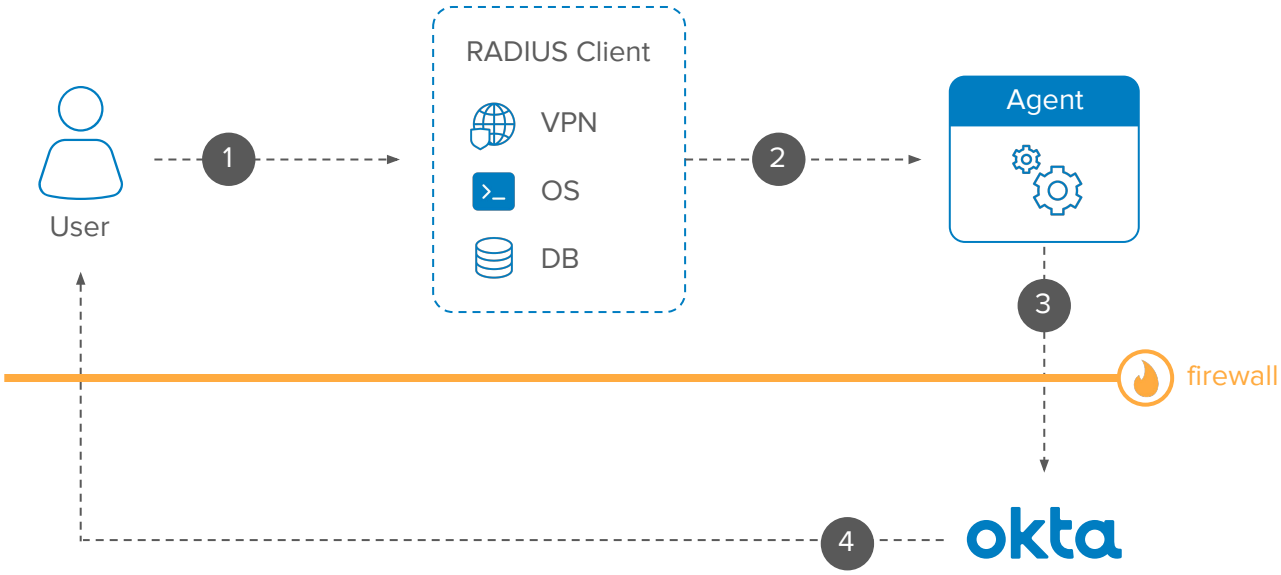
| | Read data from Okta | Write data to Okta | Read data from a 3rd party system | Write data to a 3rd party system | Just-in-Time user management (JIT) | Authentication | MFA | Authorization |
|---|---|---|---|---|---|---|---|---|
| RADIUS | | | | | | ✓ | ✓ | |
| LDAP Cloud Interface | | | | | | ✓ | | |
| LDAP and Active Directory Synchronization | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ |
| Security Assertion Markup Language (SAML) | | | | ✓ | ✓ | ✓ | ✓ | |
| Web Services Federation (WS-Federation) | | | | ✓ | | ✓ | ✓ | |
| OAuth | | | | | | | | ✓ |
| OpenID Connect (OIDC) | | | | | ✓ | ✓ | ✓ | |
| Reverse Proxies (Header-Based authentication) | | | | | | ✓ | ✓ | ✓ |
| Secure Web Authentication (SWA) | | | | | | ✓ | ✓ | |
| System for Cross-domain Identity Management (SCIM) | ✓ | ✓ | ✓ | ✓ | | | | |
| On-Premises Provisioning (OPP) | ✓ | ✓ | ✓ | ✓ | | | | |
| Time Based One-Time Password (OATH-TOTP) | | | | | | | ✓ | |
| On-Premises MFA | | | | | | | ✓ | |
| Smart Cards and Personal Identity Verification card (PIV) | | | | | | ✓ | ✓ | |
| FIDO U2F | | | | | | | ✓ | |
| Remote Desktop Protocol (RDP) | | | | | | ✓ | ✓ | |
| Secure Shell (SSH) | | | | | | ✓ | ✓ | |
| Okta Management APIs (REST APIs) | ✓ | ✓ | | | | ✓ | ✓ | |

# RADIUS

RADIUS is a legacy protocol typically used in Network Devices, Databases, and Firewalls for Authentication and MFA. Okta leverages the RADIUS protocol to support legacy systems via the Okta RADIUS Agent. The Agent is installed behind your corporate firewall and allows you to leverage Okta without exposing the RADIUS connection on the internet or requiring inbound rules in your firewall.

## Typically supported by

- VPNs and Firewalls
- Network Appliances
- Oracle Database




*RADIUS: Conceptual Diagram*

## Components

- **User**: Access and authenticate against applications compatible with RADIUS.
- **RADIUS Client**: Applications that can integrate with RADIUS as a client. During runtime, these apps capture user credentials and connect with Okta via RADIUS agent for authenticating the user.
- **Agent**: The Okta RADIUS Agent acts as a broker. It receives RADIUS requests inside your network and sends REST API requests to Okta. The agent performs outbound connections to Okta and doesn't expose RADIUS connections outside your network.
- **Okta**: Validates and processes User login and MFA via RADIUS Agent.

## Use-Cases supported

### Authentication

- Authenticate on apps that support RADIUS, such as VPNs, Firewalls, and VDIs
- Enforce MFA on apps that support RADIUS

## References

Configuring RADIUS Applications in Okta

Okta RADIUS Agent Best Practices

VPN/Network Appliance Integrations

Virtual Desktop Integrations

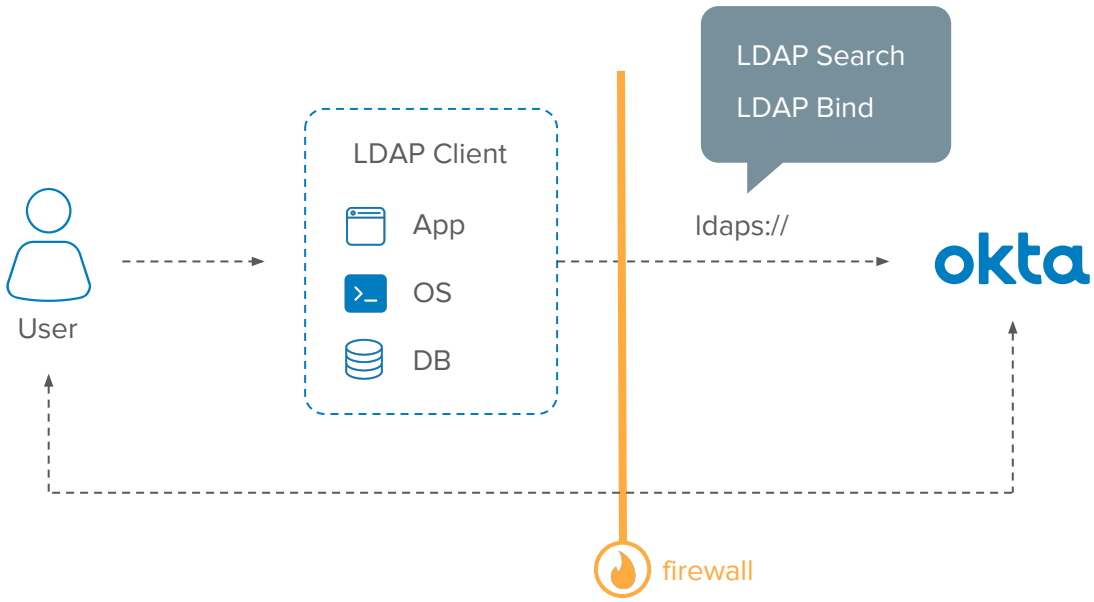
# LDAP Cloud Interface

Okta exposes users and groups as a Cloud LDAPv3 read-only directory interface, so apps can search for and authenticate identities without requiring an LDAP set on premises.

The Okta LDAP interface extends the traditional LDAP protocol with support for Multi-Factor Authentication, so users can log in using pushing notification or OTP.

## Typically supported by

- Legacy Intranet Applications and Intranet Portals
- Legacy Customer Web Applications




*LDAP Interface: Conceptual Diagram*

## Components

- **User**: Access and authenticate against applications compatible with LDAP.
- **LDAP Clients**: Applications that can integrate with LDAP as a client. During runtime, these apps capture user credentials and connect with Okta via LDAPS for authenticating the user.
- **Okta**: Provides an LDAPS interface over the cloud. During runtime, receives requests from the LDAP clients to authenticate users. The authentication may contain an OTP or a request for Push notification. Okta can deliver push notifications for end-users via Okta Verify.
- **Firewall**: The client application can be located on the intranet and protected by a Firewall, as long as it can make outbound connections to your Okta tenant (i.e., https://org.okta.com) via port 443.

## Use-Cases supported

### Read data from Okta

- Access user and group data from Okta in LDAP format
- Provide an LDAP store for external clients such as Cisco Umbrella, Atlassian Confluence, Atlassian Jira, and JFrog Artifactory

### Authentication

- Authenticate users via LDAP
- Authenticate users via LDAP with Multi-Factor Authentication

## References

Seamlessly Connect to your existing User Store with LDAP Interface

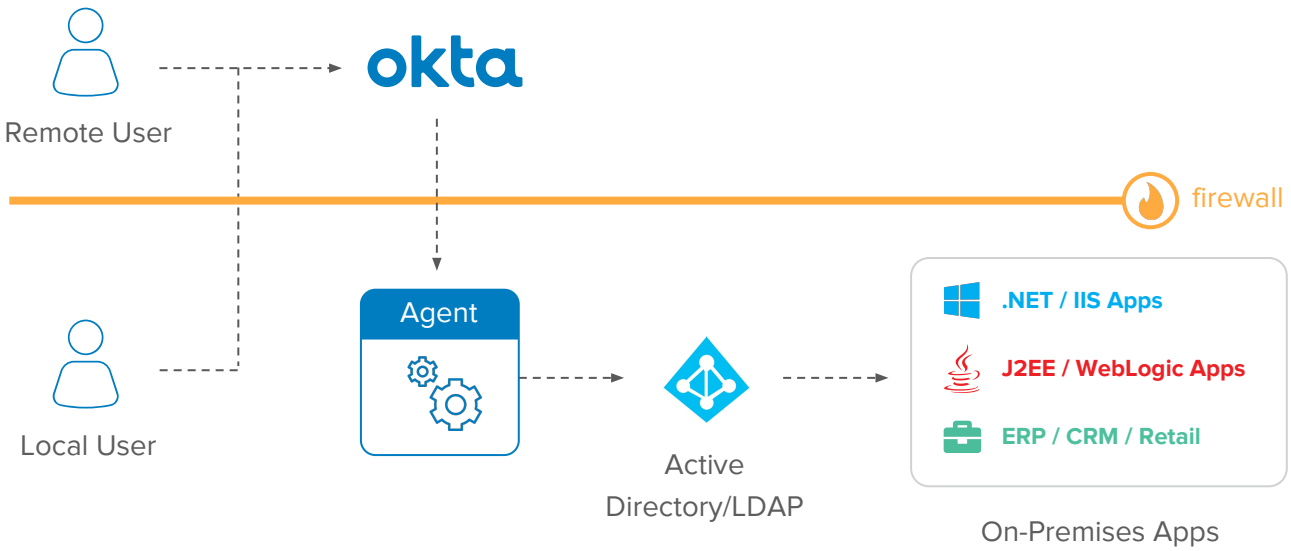
# LDAP and Active Directory Synchronization

Okta integrates with your existing LDAPv3 directories such as Active Directory, OpenLDAP, Sun One, and Oracle Internet Directory so you can import users and groups, delegate authentication, change passwords, or manage identities and groups from Okta to your LDAP.

Okta supports integrating with multiple LDAP domains and instances at the same time. This integration is typically used on complex AD environments with multiple domains and for merging environments, saving time and money – especially during M&A and IT consolidation projects. The LDAP and AD integration leverage an agent that is deployed in your intranet and doesn't require inbound connections configured in your firewall.

## Typically supported by

- Active Directory
- LDAPv3 compliant servers such as Oracle Internet Directory, Sun One, OpenDJ, and OpenLDAP.




*LDAP/AD Sync: Conceptual Diagram*

## Components

- **Local and Remote users**: Okta supports different types of user in parallel, and you can consolidate both users from LDAP/AD and external users.
- **Active Directory/LDAP**: Directory store for users and groups.
- **On-Premises Apps**: Apps that leverage the directory services provided by either AD or LDAP on-premises. After integrating your Directory with Okta, these services benefit from the directory synchronization capabilities offered by Okta.
- **Okta**: Sync user and group data with Active Directory and authenticate Local Users in Active Directory.
- **Agent**: Agent used to proxy the communication between Okta and Active Directory/LDAP on user imports and for user logins.
- **Firewall**: The LDAP/AD agent is deployed on your network and protected by a Firewall. The Firewall doesn't require extra rules for inbound connections.

## Use-Cases supported

**Read data from AD and LDAP**

- Import users and groups from LDAP and Active Directory to Okta
- Support Active Directory in Multi-Forest/Multi-Domain scenarios
- Support multiple LDAP domains and Multi-Master Replication scenarios

**Just-in-Time user management (JIT)**

- Import and Update LDAP or AD users in Okta real-time in a successful login.

**Write data to LDAP and AD**

- Write users and groups in LDAP and AD
- Reset Password on LDAP and AD
- Consolidate LDAP and AD domains
- Support Active Directory in Multi-Forest/Multi-Domain scenarios
- Support multiple LDAP domains

**Authentication**

- Delegate User Authentication to LDAP and AD
- Leverage Active Directory Desktop Single Sign-On

**Authorization**

- Leverage LDAP / AD groups for access control in Okta

## References

Okta Directory Integration: An Architecture Overview

# Security Assertion Markup Language (SAML)

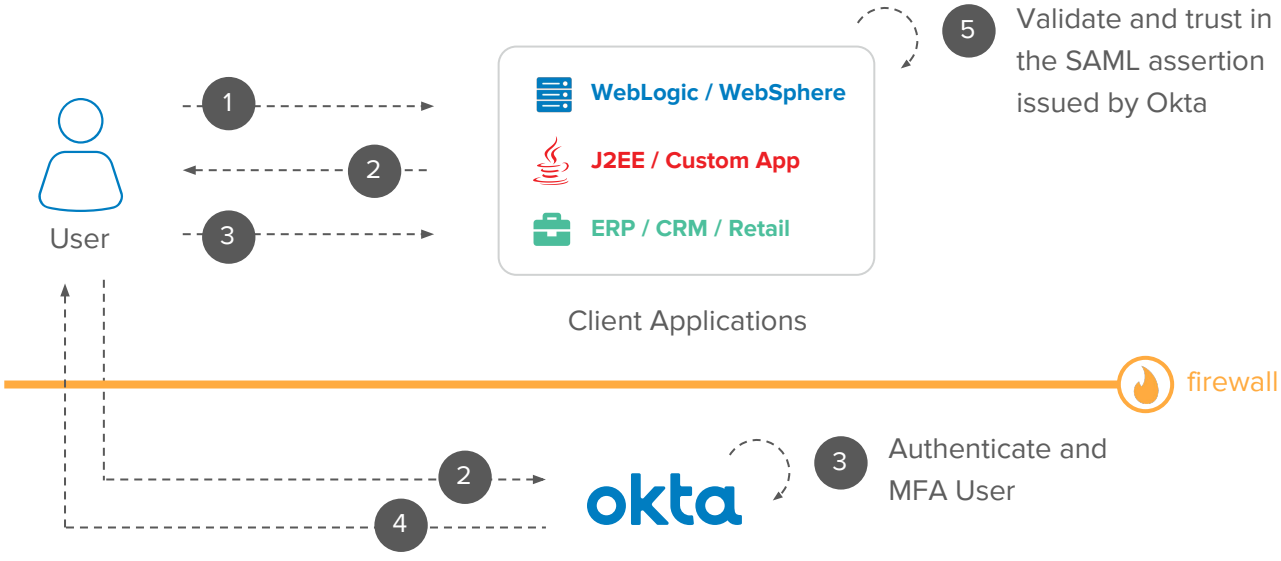
Security Assertion Markup Language (SAML) is an XML-based protocol used for Single Sign-On (SSO) and for exchanging authentication and authorization data between apps. SAML is the most popular standard used for cross-domain single sign-on (SSO).

Okta supports integrating with SAML 2.0 apps as an Identity Provider (IdP) – provides SSO to 3rd party apps – and as a Service Provider (SP) – consume SSO from other SSO solutions. Okta also supports integrating with SAML 1.0 as an Identity Provider (IdP).

## Typically supported by

- J2EE Application Servers such as WebLogic and WebSphere
- HTTP Servers such as Apache
- Load Balancers and WAN appliances such as Big-IP F5 and Akamai
- 3rd party SSO solutions such as Oracle Access Manager, CA SiteMinder, IBM Tivoli, and ADFS.

## Okta as Identity Provider (SAML-IdP)

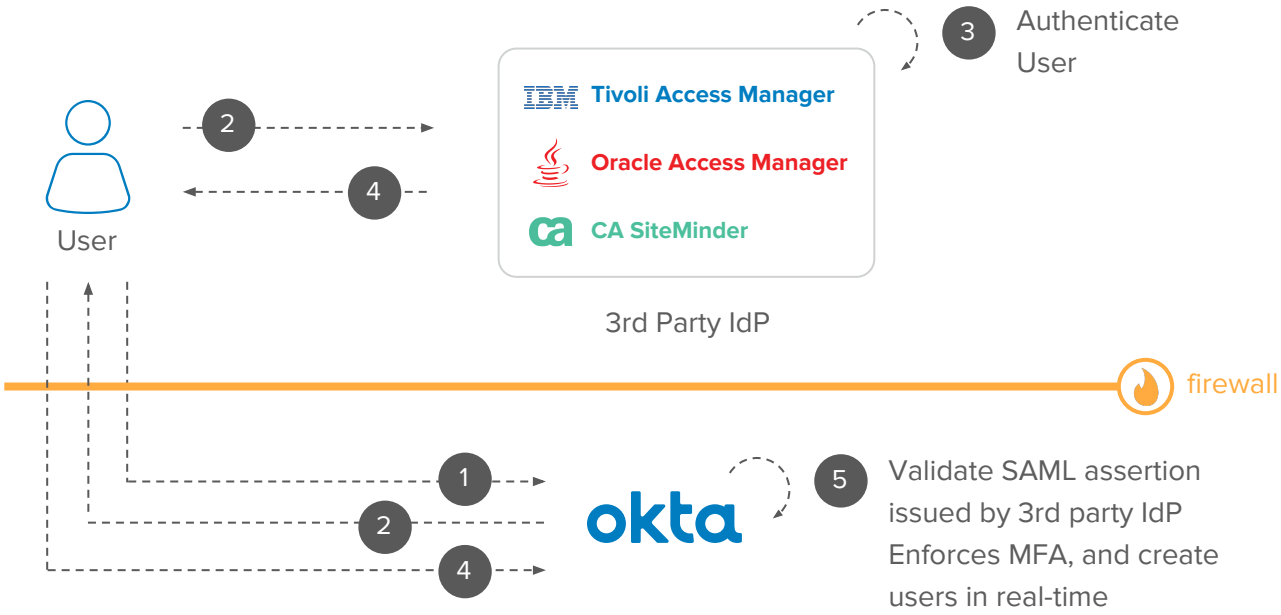



*SAML: Okta as Identity Provider: Conceptual Diagram*

## Components

- **User**: Access applications protected by Okta via SAML.
- **Client Applications**: Act as a SAML Service Provider (SAML-SP) and delegate the user authentication to Okta. Validate SAML assertions from Okta to establish the user session.
- **Okta**: Act as a SAML Identity Provider (SAML-IdP). Provides Multi-Factor Authentication and Single Sign-On for the end-user and send SAML assertions to the client application.
- **Firewall**: The user and client applications can be located on your intranet and protected by a Firewall, as long as the end-user can reach Okta through the internet.

## Okta as Service Provider (SAML-SP)




*SAML: Okta as Service Provider: Conceptual Diagram*

## Components

- **User**: Launch Okta to Single Sign-On into Cloud and On-Premise Apps.
- **Okta**: Act as a SAML Service Provider (SAML-SP) and delegate the user authentication to the 3rd party IdP. Validate SAML assertions from Okta to establish the user session. Can implement Multi-Factor authentication on top of the 3rd party login to establish the session.
- **3rd party IdP**: Act as a SAML Identity Provider (SAML-IdP) for Okta. Authenticate users and send SAML assertions back to Okta.
- **Firewall**: The 3rd party IdP can be located on your intranet and protected by a Firewall, as long as the end-user can reach Okta through the internet.

## Use-Cases supported

### Authentication

- Integrate as Identity Provider and Service Provider
- Provide Multi-Factor Authentication and SSO for custom apps.
- Route users for 3rd party IdP SSO based on Network, user email, and other contextual information.

### Just-in-Time user management (JIT)

- Import and Update 3rd party IdP users in Okta real-time in a successful login
- Receive custom attributes from 3rd party IdP

### Write data to Legacy App

- Support Just in Time provisioning (JIT) as IdP
- Send custom attributes to Service Provider

## References

Beginner's Guide to SAML

Okta SAML Integration Documentation

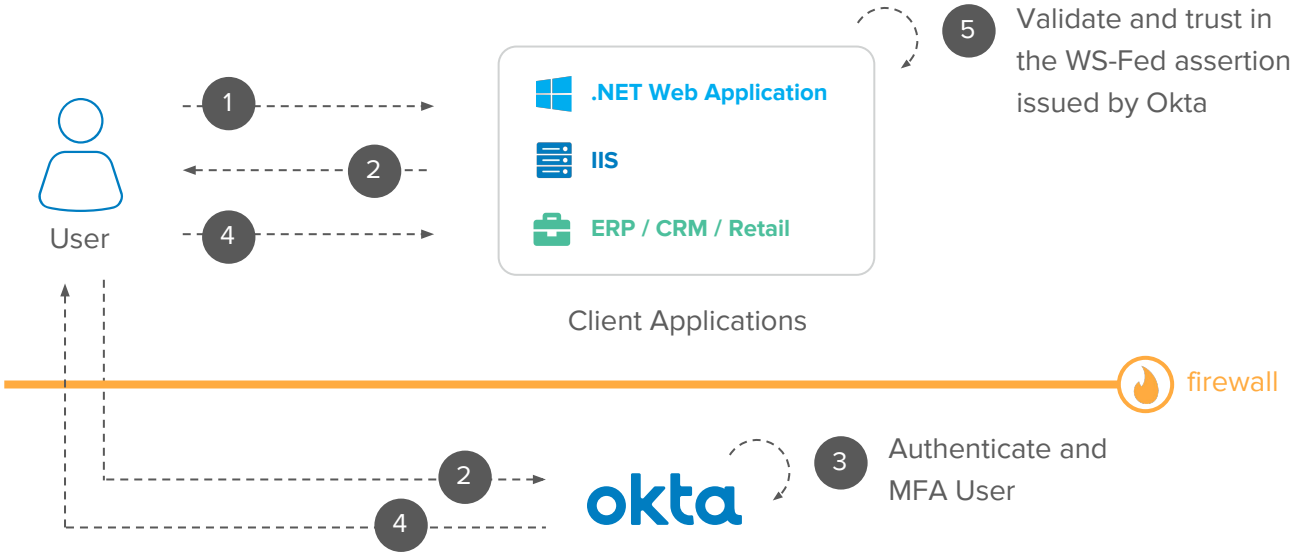
# Web Services Federation (WS-Federation)

**Tip**: *The WS-Federation architecture and conceptual diagrams are similar to the SAML integration.*

Web Services Federation – also known as WS-Federation or WS-Fed – is an XML-based protocol used for Single Sign-On and Identity Federation. The WS-Fed standard is typically used on legacy Windows Web Applications and by popular Windows SaaS services such as Office 365, which is natively supported by Okta. Okta supports integrating with WS-Fed applications as an Identity Provider (IdP).

## Typically supported by

- Microsoft Web Applications built in ASP.NET




*WS-Fed: Conceptual Diagram*

## Components

- **User**: Access applications protected by Okta via WS-Fed.
- **Client Applications**: Act as a WS-Fed Service Provider (SP) and delegate the user authentication to Okta. Validate WS-Fed assertions from Okta to establish the user session.
- **Okta**: Act as a WS-Fed Identity Provider (IdP). Provides Multi-Factor Authentication and Single Sign-On for the end-user and send WS-Fed assertions to the client application.
- **Firewall**: The user and client applications can be located on your intranet and protected by a Firewall, as long as the end-user can reach Okta through the internet.

## Use-Cases supported

### Authentication

- Integrate as Identity Provider
- Provide Multi-Factor Authentication and SSO for custom apps.

### Write data to Legacy App

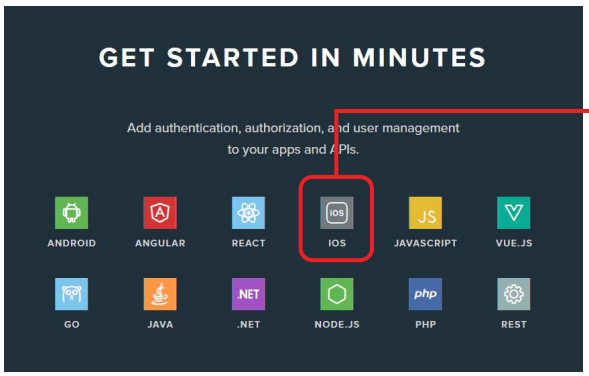
- Support Just in Time provisioning (JIT) as IdP
- Send custom attributes to Service Provider

## References

Configuring WS Federation apps in Okta

# OAuth

OAuth is an HTTP-based standard used for API authorization on modern applications and microservices. Okta supports OAuth as an Authorization Server and can control access to APIs. Okta also provides SDKs for 11 of the most popular programming languages, which accelerates the development process.



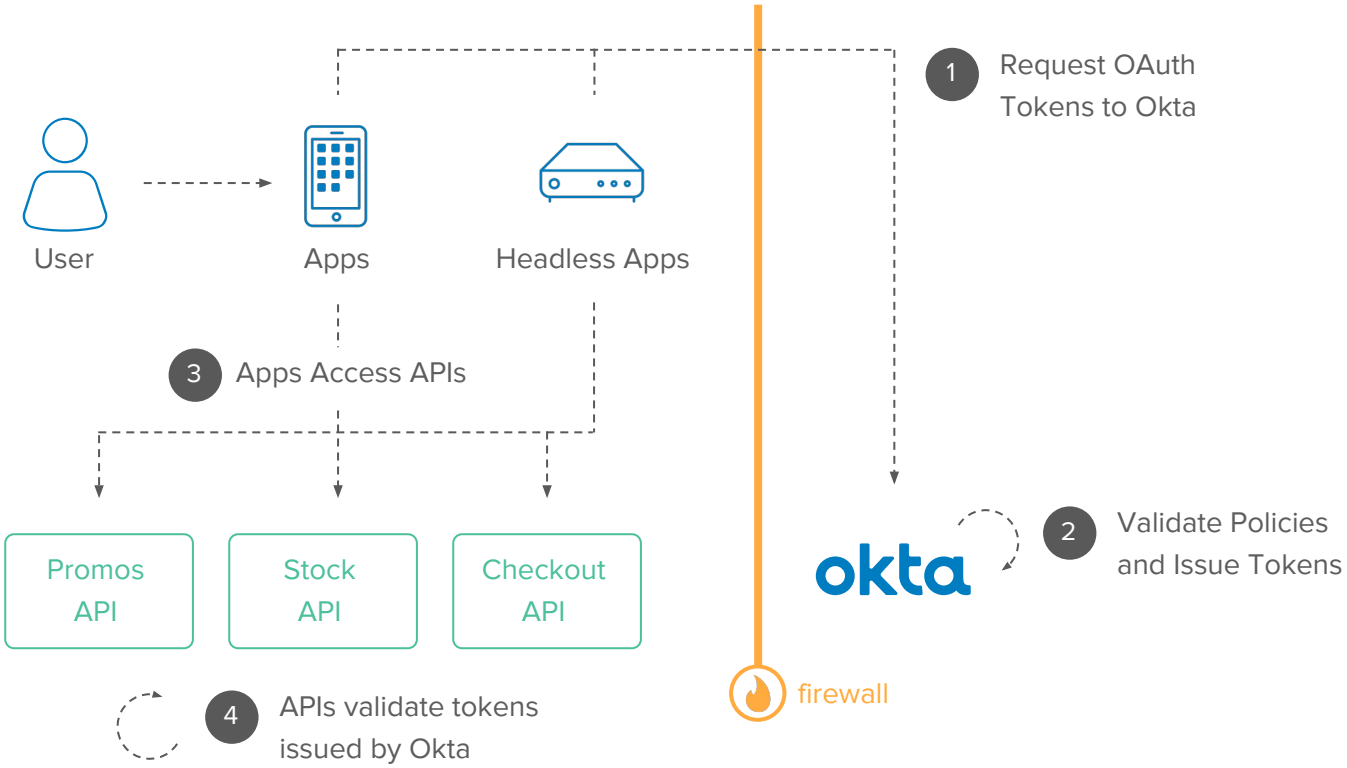

Select SDK


Try code sample and implement app

*To simplify integrations, Okta Supports SDKs and Code Samples.*

## Typically supported by

- Modern Web and Mobile Apps
- Microservice Apps
- Modern Headless Apps
- API Gateways
- SOA and BPM solutions




*OAuth App: Conceptual Diagram*

## Components

- **User**: Accesses modern applications integrated with Okta via OAuth and OpenID Connect.
- **Apps (Mobile and Headless)**: Request OAuth tokens to Okta.
- **Okta**: Processes API authorization requests and issues OAuth tokens and scopes.
- A**PIs (i.e., Promos, Stock, and Checkout):** Receive requests from Apps containing OAuth tokens. Validate tokens issued by Okta to confirm the access.
- **Firewall**: Typically, modern applications and APIs are exposed on the Internet. However, Okta also supports OAuth applications located on the intranet and protected by your Firewall.

## Use-Cases supported

### Authentication

- Authenticate and MFA users to access custom apps (in conjunction with OpenID Connect)

### Authorization

- Provide Authorization for Mobile Apps, Web Apps, Microservices, and headless clients
- Work as an Authorization Server for custom apps
- Issue custom scopes and claims
- Support Refresh Tokens
- Support Dynamic Client Registration

## References

Okta Developers Documentation Index

Postman Collections (include OAuth collections)

Okta's API Access Management

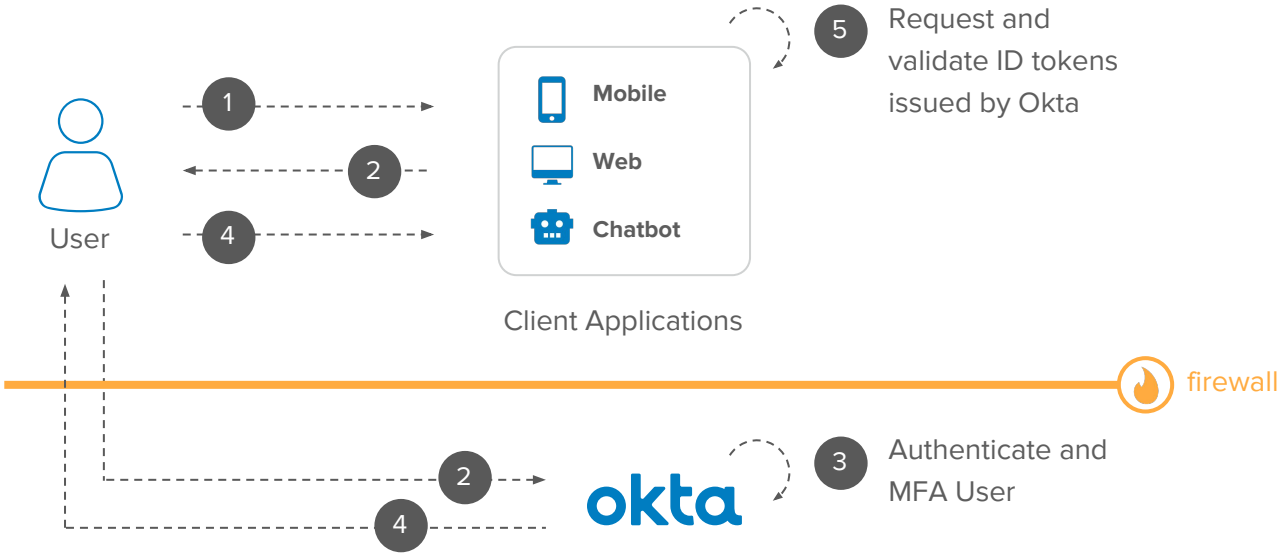
# OpenID Connect (OIDC)

OpenID Connect is a standard built on top of OAuth for Single Sign-On and Federation. It provides a functionality similar to SAML but tailored for modern applications and Microservices. Okta supports integrating with OpenID Connect apps as an Authorization Server/Identity Provider (IdP) and as a Client App/Service Provider (SP).

## Typically supported by

- Social Networks such as Google Plus
- Modern Web and Mobile Apps
- Microservice Apps
- HTTP Servers such as Apache and NGINX
- CDNs such as Cloudflare

## Okta as Authorization Server

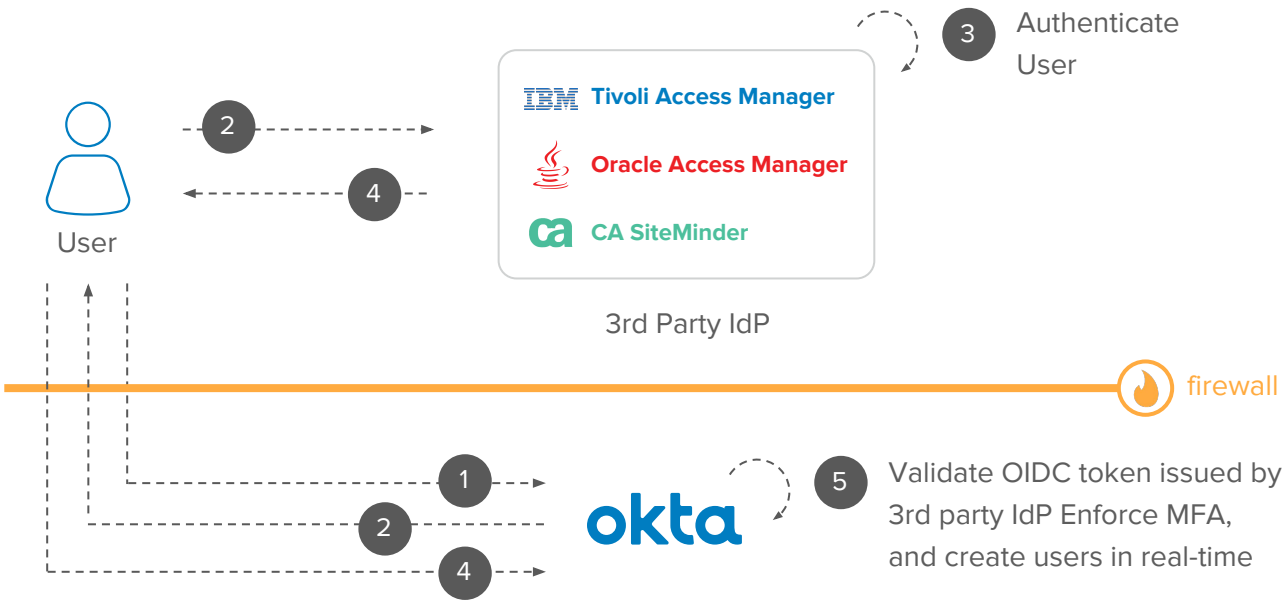



*OpenID Connect: Okta as an Authorization Server: Conceptual diagram*

## Components

- **User**: Access applications protected by Okta via OpenID Connect.
- **Client Applications**: Act as an OIDC Client Application and delegates the user authentication to Okta. Obtain an ID token from Okta to establish the user session.
- **Okta**: Act as an OIDC Authorization Server. Provides Multi-Factor Authentication and Single Sign-On for the end-user to grant access to the client application.
- **Firewall**: Typically, modern applications and APIs are exposed on the Internet. However, Okta also supports OIDC Client Apps located on the intranet and protected by your Firewall.

## Okta as a Client Application




*OpenID Connect: Okta as a Client App: Conceptual diagram*

## Components

- **User**: Access Okta.
- **Okta**: Act as an OIDC Client App and delegate the user authentication to the 3rd party Authorization Server. Obtain an ID token to establish the user session. Can implement Multi-Factor authentication on top of the 3rd party Authorization Server to establish the session.
- **3rd party IdP**: Act as an OIDC Authorization Server for Okta. Authenticate users and send id_tokens with claims back to Okta.
- **Firewall**: Most OIDC Authorization Servers are exposed on the Internet. However, Okta also supports OIDC Authorization Servers located on the intranet and protected by your Firewall.

## Use-Cases supported

### Authentication

- Integrate as Authorization Server and Client App
- Provide Multi-Factor Authentication and SSO for custom modern apps.
- Route users for 3rd party Authorization Server based on Network, user email, and other contextual information.
- Implement MFA on top of the 3rd party OIDC Authorization Server

### Just-in-Time user management (JIT)

- Import and Update 3rd party IdP users in Okta real-time in a successful login
- Support Just in Time provisioning (JIT) as Client Application
- Receive custom claims from 3rd party Authorization Server
- Support Social Authentication

### Write data to Legacy App

- Support Just in Time provisioning (JIT) as Authorization Server
- Send custom claims to the Client Application

## References

Authentication with Okta

Sign-In your users with OpenID Connect

# Reverse Proxies (Header-Based authentication)

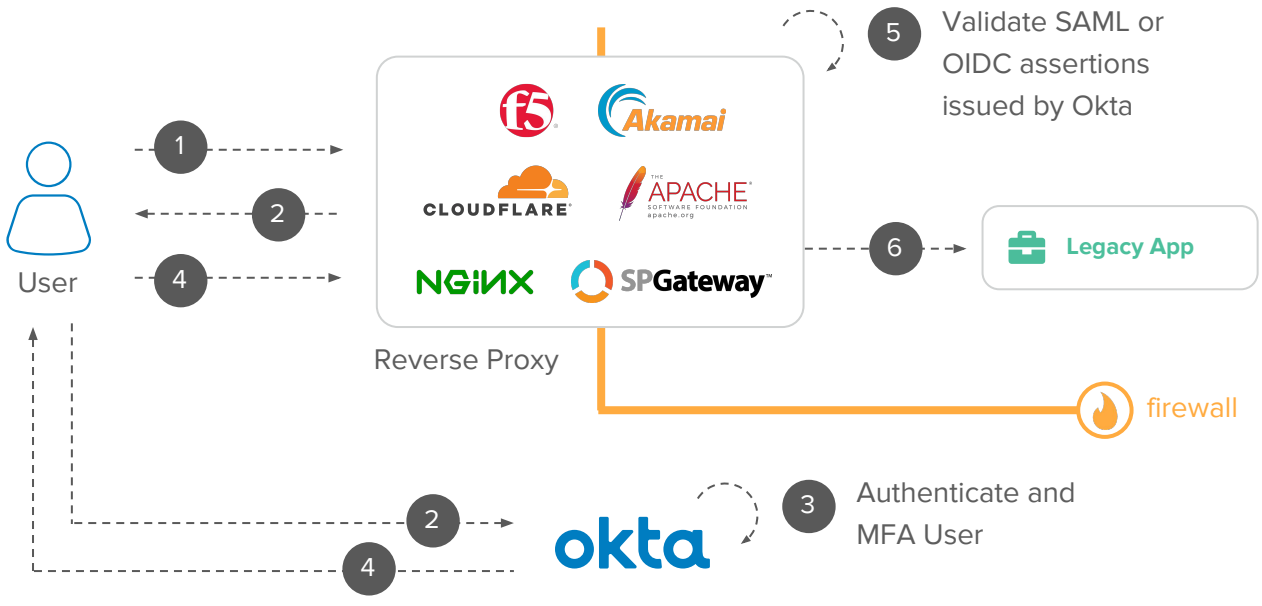
Header-based Authentication is a Web Access Management strategy used by legacy Single Sign-On solutions to secure web apps with perimeter security. It implements SSO authentication and enforcement on a Load Balancer or HTTP server that works as the only access point between end-users and intranet apps.

The Load Balancer/HTTP server intercepts all the user HTTP requests and validates the user session. If the session is valid, the server allows the request to reach the application on the intranet and adds an HTTP header variable with the userid so the application can identify who is authenticated.

Okta supports integrating with CDNs, HTTP Servers, and Load Balancers – such as Apache, NginX, ICSynergy SPGateway, Akamai, F5 Big-IP, and CloudFlare – that support header-based authentication.

## Typically supported by

- Load Balancers and WAN appliances such as Big-IP F5 and Akamai
- HTTP Servers such as Apache, NGINX, and ICSynergy SPGateway.
- CDNs such as CloudFlare Access.




*Reverse Proxy with Header-Based Authn: Conceptual Diagram*

## Components

- **User**: Access legacy applications that served by the Reverse Proxy.
- **Reverse Proxy**: Load Balancer, HTTP Server, or CDN solution that act as a SAML Service Provider or an OIDC Client Application and delegates the user authentication to Okta. After authentication, the reverse proxy can leverage the assertion information to enforce authorization.
- **Okta**: Act as an OIDC Client App and delegate the user authentication to the 3rd party Authorization Server. Obtain an ID token to establish the user session. Can implement Multi-Factor authentication on top of the 3rd party Authorization Server to establish the session.
- **Legacy Applications**: Application that receives user requests via Reverse Proxy. The legacy application captures the user id from the HTTP header to establish an app session.
- **Firewall**: For security reasons, companies using this pattern must limit access to the legacy applications only via the Reverse Proxy.

## Use-Cases supported

**Read data from Okta**

- Fill internal HTTP headers with information from Okta

**Authentication**

- Authenticate and MFA users in Okta

**Authorization**

- Reverse Proxy can use the assertion information to enforce authorization

## References

Okta Integration Guide for Web Access Management with F5 Big-IP

Replace your complicated VPN with Cloudflare Access and Okta

Integrate Okta with Akamai Enterprise Application Access

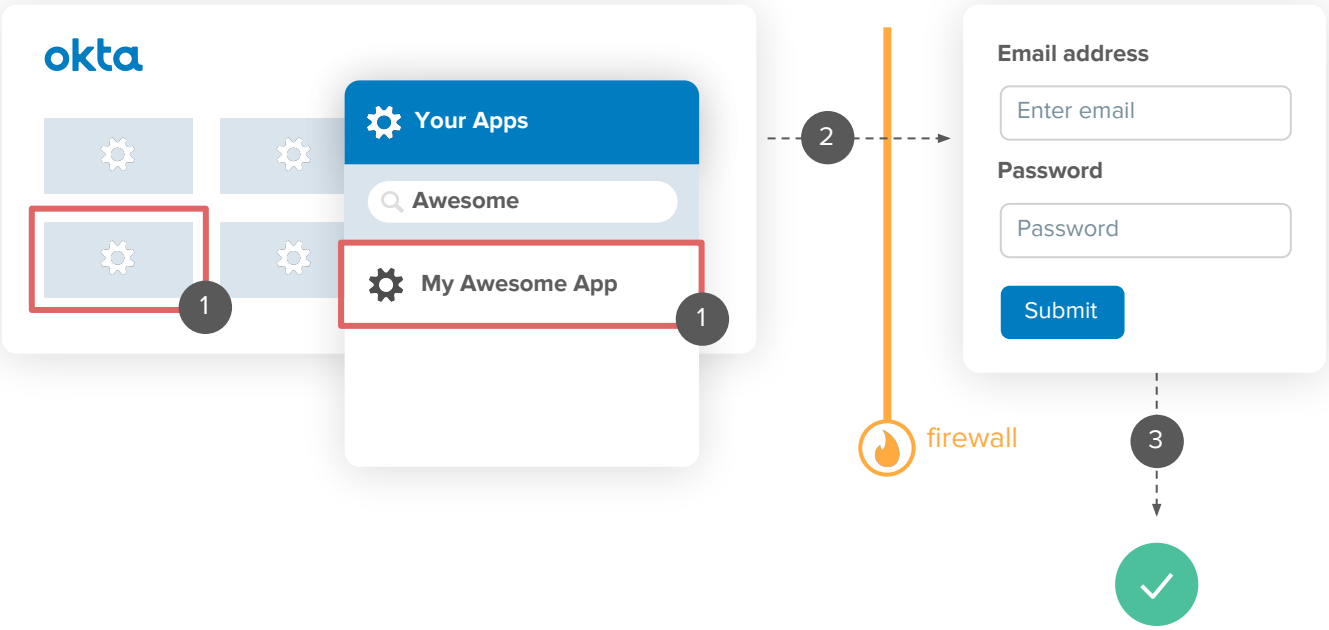
# Secure Web Authentication (SWA)

Secure Web Authentication (SWA) is an Okta technology used for providing Single Sign-On to web applications that do not support federation protocols such as SAML, WS-Fed, and OpenID Connect.

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, they 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 (form-fill).

## Typically supported by

- Legacy Web Applications with login forms and that don't support SAML, WS-Fed, or OpenID Connect.




*SWA: Conceptual Diagram*

## Components

- **User**: Launch the application via the Okta Home, the Okta SWA Plugin, or by visiting the website.
- **Okta Plugin**: Validates the website access, fetch credentials from Okta and performs the authentication on behalf of the user.
- **Firewall**: The integrated app can be located on the intranet and protected by a Firewall.
- **App**: Validates and processes the authentication and displays the logged page to the end-user.

## Use-Cases supported

### Authentication

- Provide SSO to applications that do not support federation protocols.
- Require MFA from users in order to log into legacy apps.
- Share access to legacy apps

## References

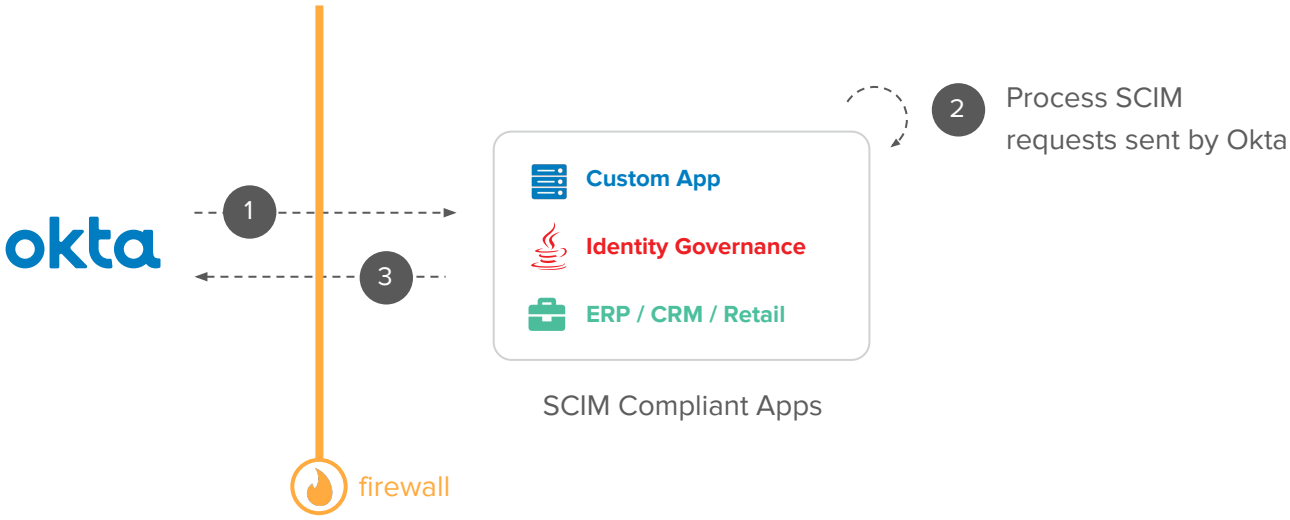
How Okta integrates applications.

# System for Cross-domain Identity Management (SCIM)

The System for Cross-domain Identity Management (SCIM) standard allows you to integrate custom applications with Okta to either manage users and groups in Okta or to leverage Okta's group and user management. The integration with Okta streamlines and automate the process of managing user accounts, credentials, and privileges on 3rd party systems. The Okta SCIM integration is provided both via a direct cloud connection or via an agent sitting on-premises.

## Typically supported by

- Web Applications with user management functions
- Identity Governance solutions




*SCIM: Conceptual Diagram*

## Components

- **Okta**: Send SCIM requests to target applications. The requests can be for importing or writing user and group data into the application.
- **SCIM Compliant Apps**: Applications that are SCIM compliant. Receives and process SCIM requests from Okta.
- **Firewall**: SCIM Applications can be accessed publicly or be deployed on the intranet and protected by a Firewall. To access the SCIM endpoint, Okta requires an inbound connection to the SCIM Application. For a connection without inbound firewall rules, check the on-premises provisioning agent.

## Use-Cases supported

**Read data from 3rd party systems**

- Use custom app as a source of truth for user accounts (profile master)
- Use custom app as a source of truth for user attributes (attribute master)
- Use custom app as a source of truth for groups (group master)
- Import custom attributes from external sources of truth

**Import user and group data to Okta**

- Manage users – provision, update, remove – on custom app
- Manage groups – provision, update, change membership, remove – on custom apps (group push)
- Support custom attributes for provisioning

## References

What is SCIM?

SCIM Provisioning with Okta's Lifecycle Management

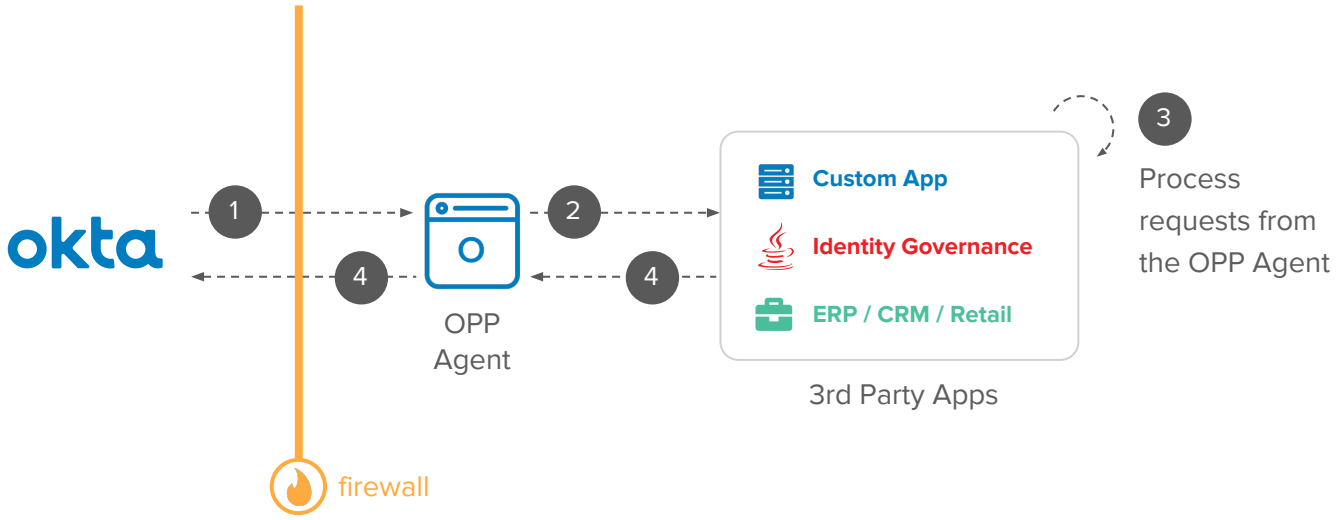
# On-Premises Provisioning (OPP)

The Okta On-Premise Provisioning (OPP) integration is used for integrating Okta with on-premises applications behind the corporate firewall without requiring inbound communication to the intranet.

The OPP integration leverages the SCIM protocol and offers capabilities similar to the SCIM integration. The communication between Okta the on-premises applications occurs through the Okta OPP Agent and a SCIM server or a provisioning connector built using Provisioning Connector SDK.

## Typically supported by

- Applications behind the corporate firewall
- Applications that do not support SCIM natively provides a Java SDKs or REST API for managing users.




*On-Premises Provisioning: Conceptual Diagram*

## Components

- **OPP Agent**: Act as a proxy for Okta in your intranet. Regularly connects to your Okta org to fetch SCIM requests and translate requests to internal applications.
- **Okta**: Import and provision user and group data to target applications proxied by the OPP Agent. The requests can be for importing or writing user and group data into the application.
- **3rd party apps**: Receives and process requests from the OPP Agent.
- **Firewall**: The OPP agent is deployed behind your corporate firewall and doesn't require inbound connections to work. For integrations with public systems, check the SCIM integration.

## Use-Cases supported

**Read data from 3rd party systems**

- Use custom app as a source of truth for user accounts (profile master)
- Use custom app as a source of truth for user attributes (attribute master)
- Use custom app as a source of truth for groups (group master)
- Import custom attributes from external sources of truth

**Import user and group data to Okta**

- Manage users – provision, update, remove – on custom app
- Manage groups – provision, update, change membership, remove – on custom apps (group push)
- Support custom attributes for provisioning

## References

What is SCIM?

SCIM Provisioning with Okta's Lifecycle Management

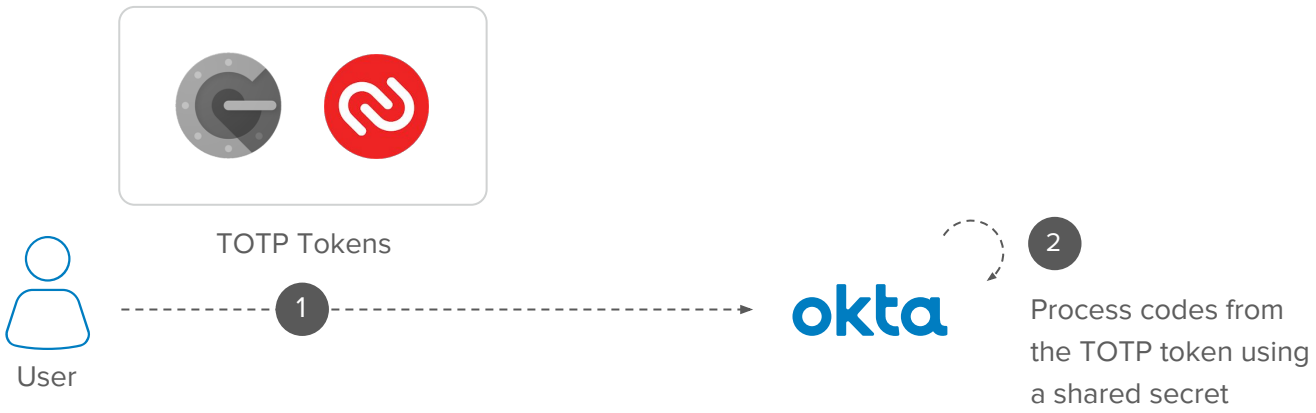
Creating SCIM connectors with Okta OPP and the Okta Connector SDK

# Time-Based One-Time Password (OATH-TOTP)

OATH TOTP is a standard implementation used for time-based MFA tokens such as Google Authenticator and Authy. Okta supports OATH-TOTP as MFA factor and you can require users to enter their TOTP keys to access systems protected by Okta.

## Typically supported by

- Google Authenticator
- Authy




*TOTP: Conceptual Diagram*

## Components

- **User**: Access Okta or a system protected by Okta.
- **Okta**: Authenticates the user and requires the code from the OATH-TOTP token for MFA.
- **TOTP token**: Generate unique codes that are validated on Okta during the authentication. The integration relies on a token seed shared between the token and Okta. Okta defines this seed during the MFA factor registration.

## Use-Cases supported

**Authentication**

- Support MFA with Google Authenticator
- Support MFA with Authy

## References

Okta Multifactor Authentication: Factors Supported

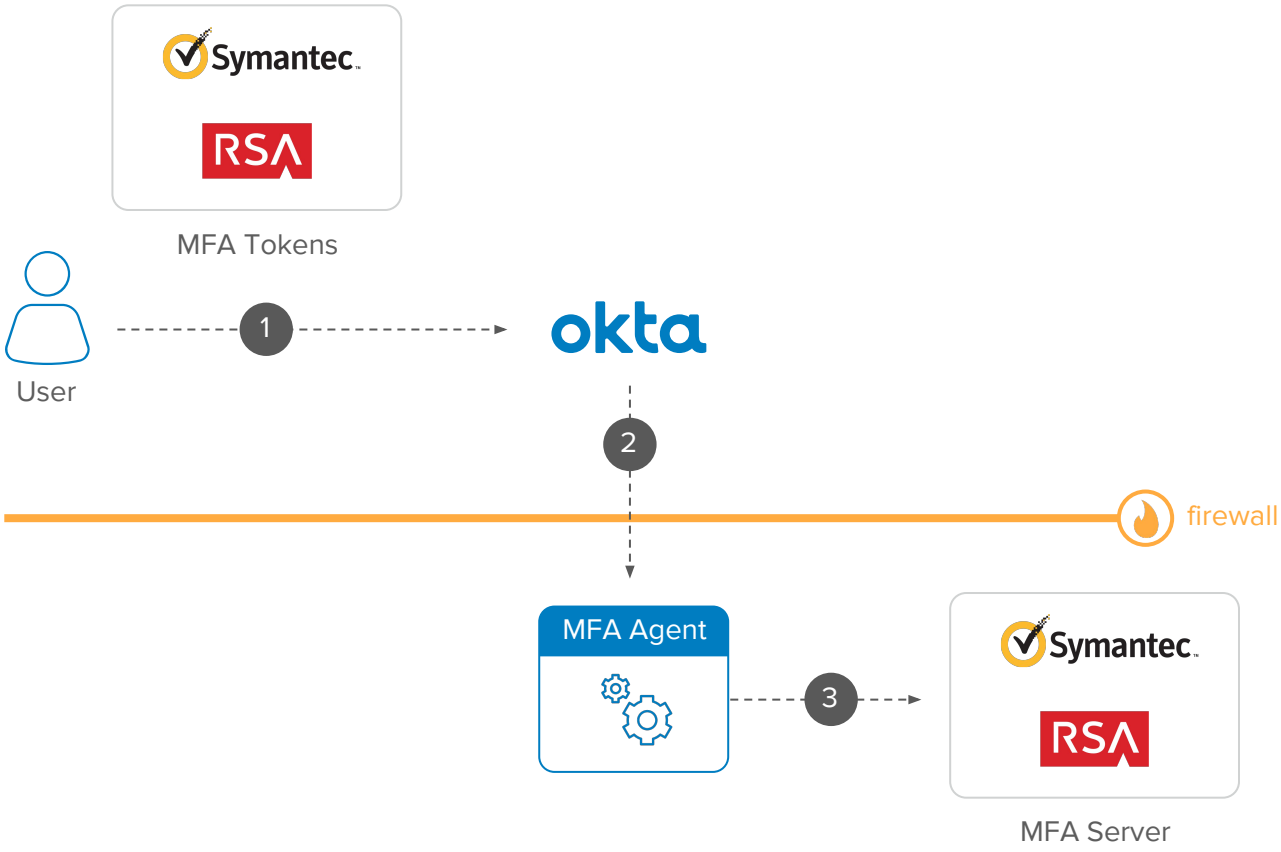
# On-Premises MFA

Okta supports integrating with legacy On-Premise MFA servers – such as RSA SecurID, VASCO, and Symantec VIP – for MFA authentication. This integration allows you to validate MFA from your on-premise server to access Okta or systems protected by Okta.

Okta integrates with On-Premises MFA using the Okta On-Prem MFA agent – formerly known as the RSA SecurID agent. This agent acts as a RADIUS client and communicates with your RADIUS-enabled on-prem MFA server.

## Typically supported by

- Legacy MFA servers with support for RADIUS clients.




*On-Premises MFA: Conceptual Diagram*

## Components

- **User**: Access Okta or a system protected by Okta.
- **Legacy MFA Token**: Generate MFA codes used for the Multi-Factor Authentication in Okta.
- **Okta**: Authenticates the user and delegates the MFA validation to the legacy MFA server.
- **Okta MFA Agent**: Act as a RADIUS proxy. Receives requests from Okta and communicates with the Legacy MFA server to validate the MFA code.
- **Legacy MFA Server**: Validates MFA codes.

## Use-Cases supported

### Authentication

- Support MFA with legacy MFA servers that supports RADIUS
- Support gradual MFA modernization/replacement.

## References

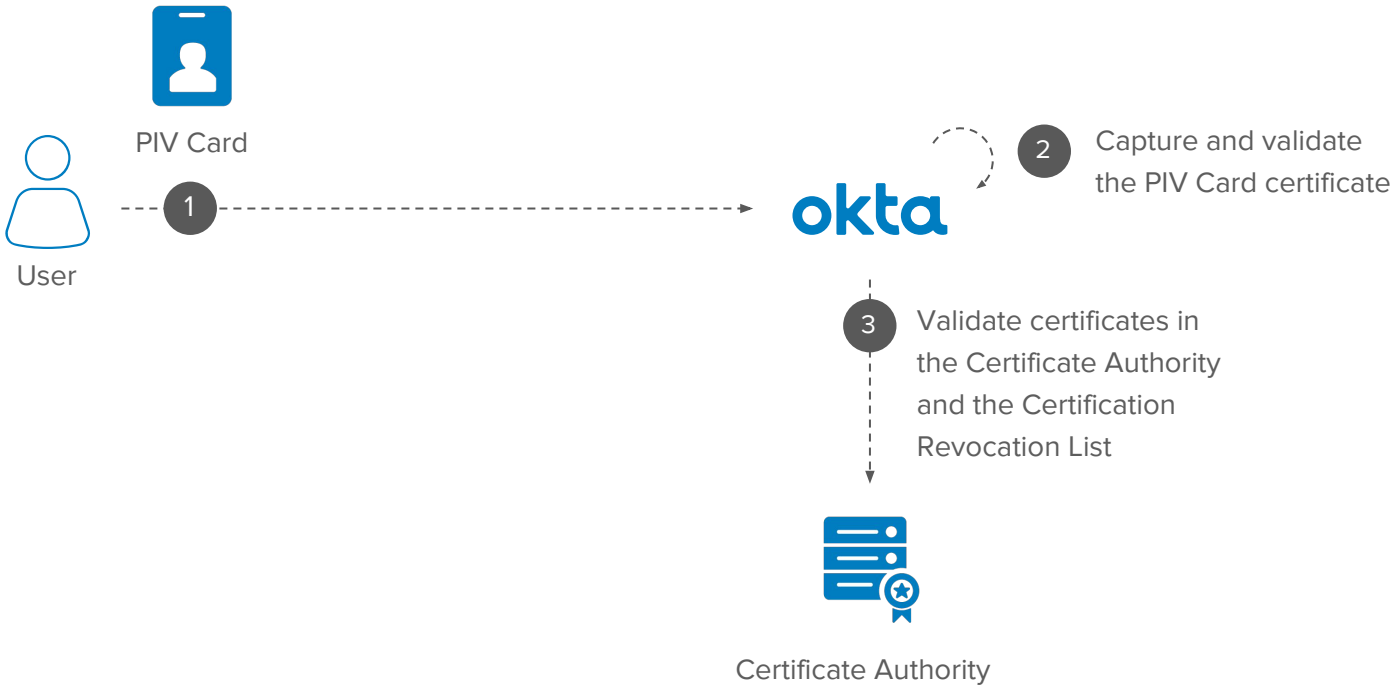
Configuring the On-Premises MFA Agent

# Smart Cards and Personal Identity Verification cards (PIV)

Smart Cards and the Personal Identity Verification (PIV) card are a form of identification typically used by government agencies for authenticating and controlling physical and logical access for employees. Okta supports X.509 certificate-based authentication to access the apps integrated with Okta.

## Typically supported by

- Federal and Government Systems
- Legacy SSO solutions on-premises




*PIV Cards: Conceptual Diagram*

## Components

- **User**: Access and log into Okta by scanning her PIV card.
- **PIV Card**: Carries a key pair and a certificate issued by a Certificate Authority (CA) used for authentication in Okta.
- **Okta**: Captures and checks the PIV certificate against the CAs trusted by the Okta administrator.
- **Certificate Authority (CA)**: Validates certificates and maintain a list of certificates that should not be trusted (Certificate Revocation List).

## Use-Cases supported

**Authentication**

- Support PIV for login
- Support multiple Cas and trust roots
- Support multiple PIV cards per user

## References

Using PIV credentials to enable Passwordless Authentication

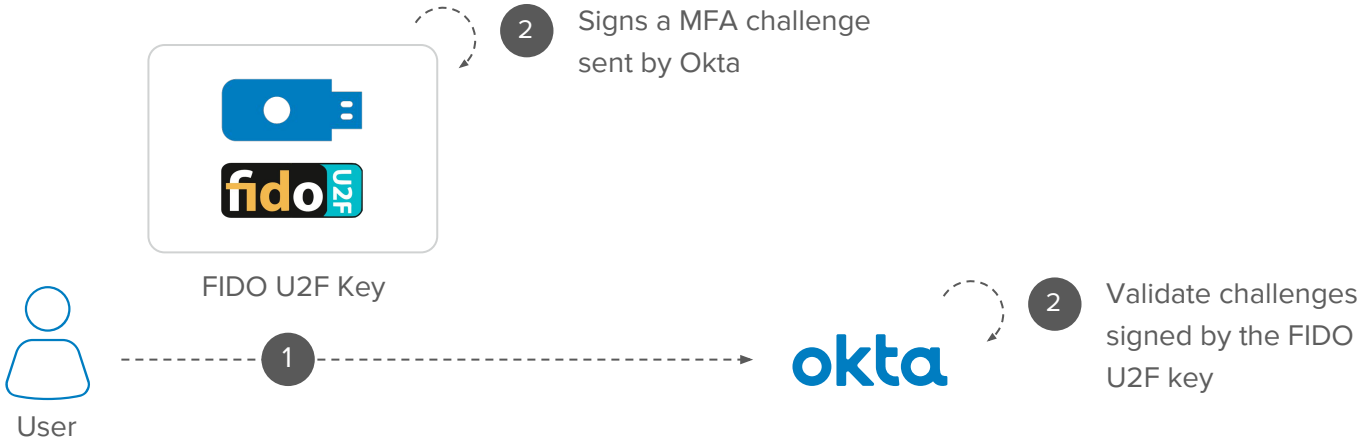
Identity Providers Supported by Okta

# FIDO U2F

FIDO U2F is a modern MFA factor used to proof the user authentication using physical tokens. Okta supports FIDO U2F tokens natively and can leverage FIDO tokens to strengthen access to legacy web apps integrated to Okta.

## Typically supported by

- Modern Web, Mobile, and Desktop Apps




*FIDO U2F: Conceptual Diagram*

## Components

- **User**: Access Okta or a system protected by Okta and uses a FIDO U2F compliant token for Multi-Factor Authentication.
- **FIDO U2F Key**: Receives challenges from Okta. Validates the user presence and signs the challenge with private keys.
- **Okta**: Validates challenges signed by the FIDO U2F key.

## Use-Cases supported

### Authentication

- Support FIDO U2F keys for MFA

## References

Okta and Yubico: Partnership

Okta MFA and FIDO U2F Keys

# Remote Desktop Protocol (RDP)

Remote Desktop Protocol (RDP) is a Microsoft protocol typically used by system administrators for accessing Windows Servers remotely. Okta provides secure access to Windows Servers in two different methods:

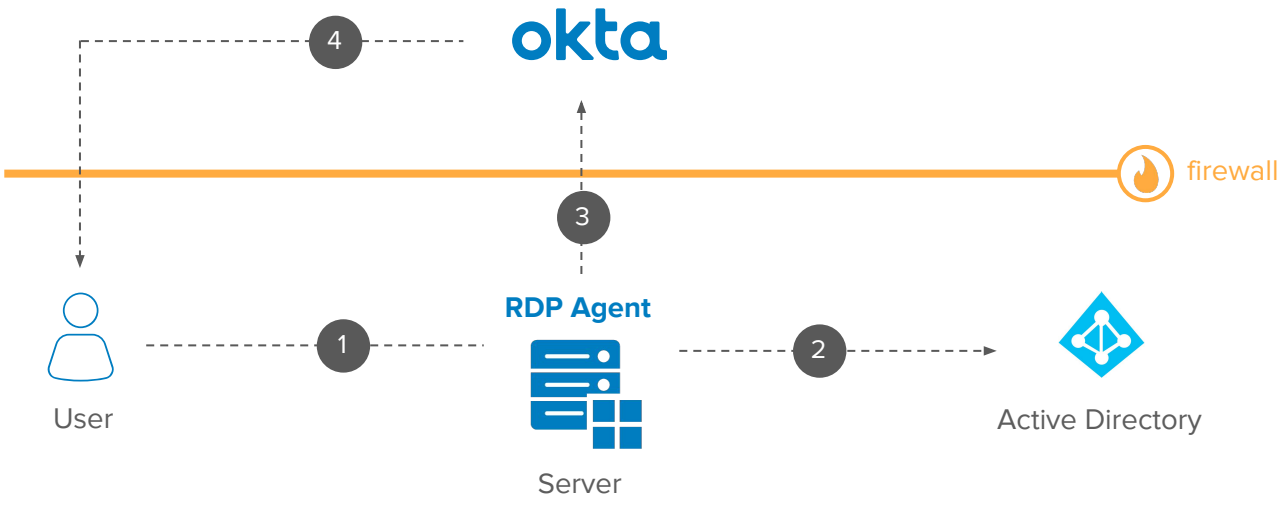
- **RDP Agent**: Provides MFA for Windows servers.
- **Advanced Server Access**: Provides ephemeral client-certificate based authentication for Windows servers. Includes additional features such as continuous device validation for clients and event audit logs.

**Tip**: *The Advanced Server Access option is great for mitigating the risk of credential misuse across cloud deployments such as Azure, GCP, and Amazon AWS.*

## Typically supported by

- Windows Servers on-premise.
- Windows Servers on Cloud providers such as Amazon AWS and Microsoft Azure.

## RDP Agent

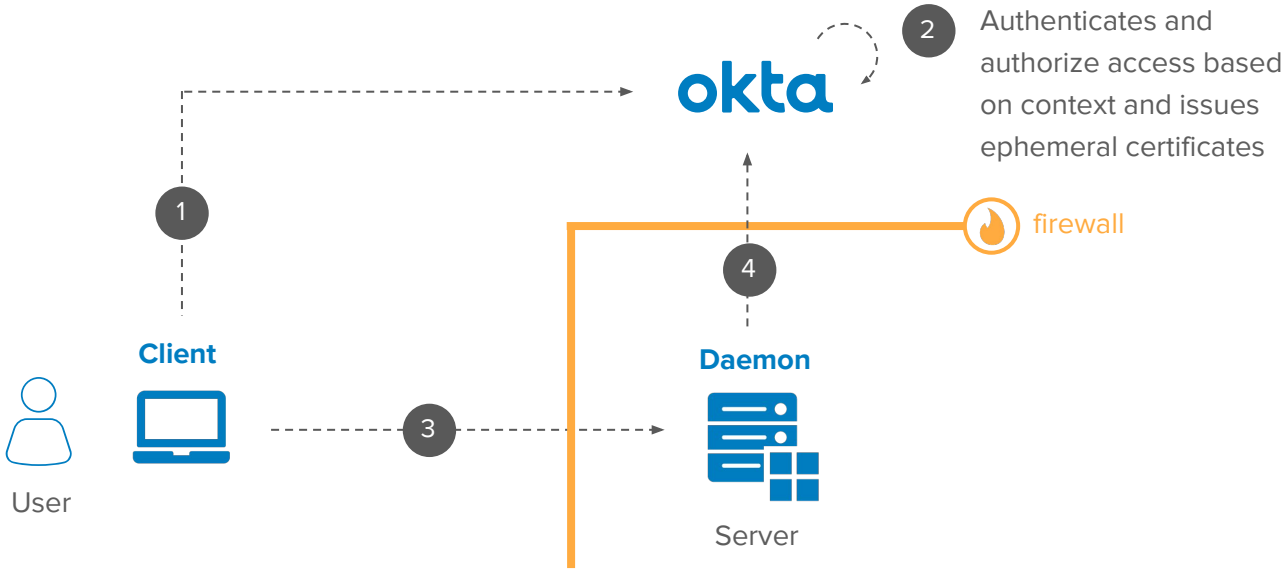



*Remote Desktop Protocol (RDP): Conceptual Diagram*

## Components

- **User**: Access a Windows Server – usually from a protected network – via Remote Desktop Protocol (RDP).
- **Server**: Windows Server accessed by User.
- **Active Directory**: Performs primary authentication with username and password.
- **RDP Agent**: The Okta RDP Agent works natively in Windows and callouts Okta for MFA.
- **Okta**: Receives requests from the RDP Agent to validate policies and extend RDP with Multi-Factor Authentication.
- **Firewall**: The windows server and the RDP connection are usually available on the intranet and protected by a Firewall. The Okta RDP agent uses only outbound connections and doesn't require firewall configuration for inbound requests. You can also use this integration to protect servers hosted in Cloud Providers.

## Advanced Server Access




*Advanced Server Access: RDP Conceptual Diagram*

## Components

- **User**: Access a Windows Server via RDP from a device with the server access client installed.
- **Server Access Client**: Communicates with Okta to establish the RDP connection. In addition, re-evaluates the access context – user, device, server – during runtime to cut off access.
- **Okta**: Receives requests from the Server Access Client. Validates user, device, and server context and issues ephemeral certificates for authentication on servers. The certificates are bound to the user, device, and server and cannot be reused.
- **Server**: Windows Server accessed by User.
- **Daemon**: Server access daemon. Implements configuration on the server side to accept ephemeral certificates issued by Okta. In addition, it manages local user accounts, audits the operating system, and regularly re-evaluates the access context during runtime to cut off access.
- **Firewall**: Both the user and the Linux server can sit on the intranet. The server can also be hosted in cloud providers and protected by a Firewall.

## Use-Cases supported

### Authentication

- Access Windows Servers with MFA provided by Okta

## References

Secure Access to your Servers with Okta MFA for RDP

Okta MFA for Servers

# Secure Shell (SSH)

Secure Shell (SSH) is a protocol used by system administrators and developers for accessing Linux and Unix servers remotely. Okta can provides secure access to Linux and Unix Servers in two different methods:

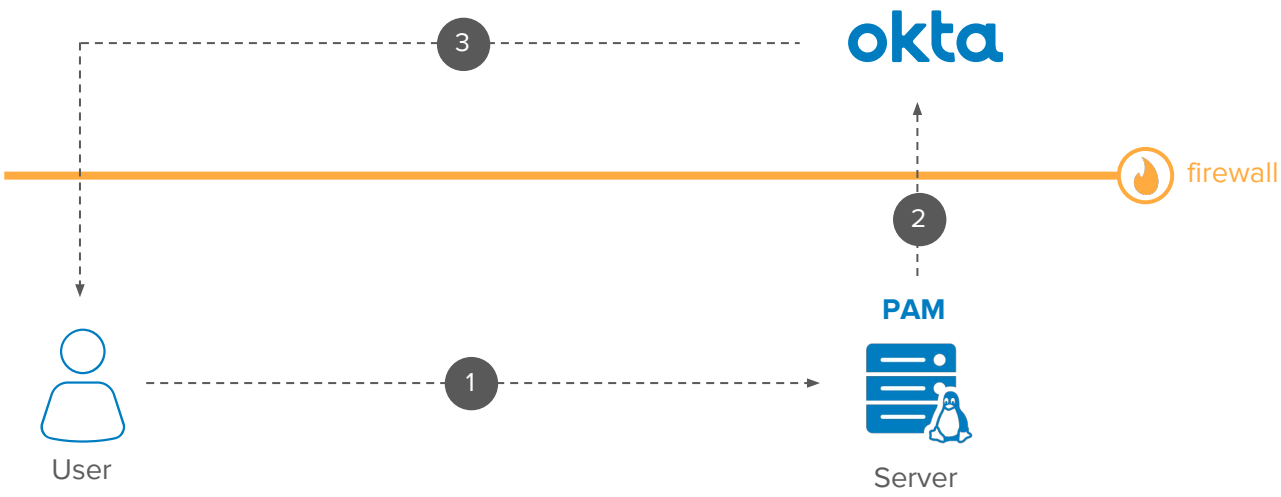
- Unix Pluggable Authentication Module (PAM): Provides basic authentication and MFA for Linux and Unix servers.
- Advanced Server Access: Provides ephemeral client-certificate based authentication for Linux and Unix servers. Includes additional features such as continuous device validation for clients, local user and group account management, and event audit logs.

**Tip**: *The Advanced Server Access option is great for mitigating the risk of credential misuse across cloud deployments such as Azure, GCP, and Amazon AWS.*

## Typically supported by

- Unix and Linux Servers on premise
- Unix and Linux Servers on Cloud providers such as Amazon AWS and Microsoft Azure.

## Pluggable Authentication Module (PAM)

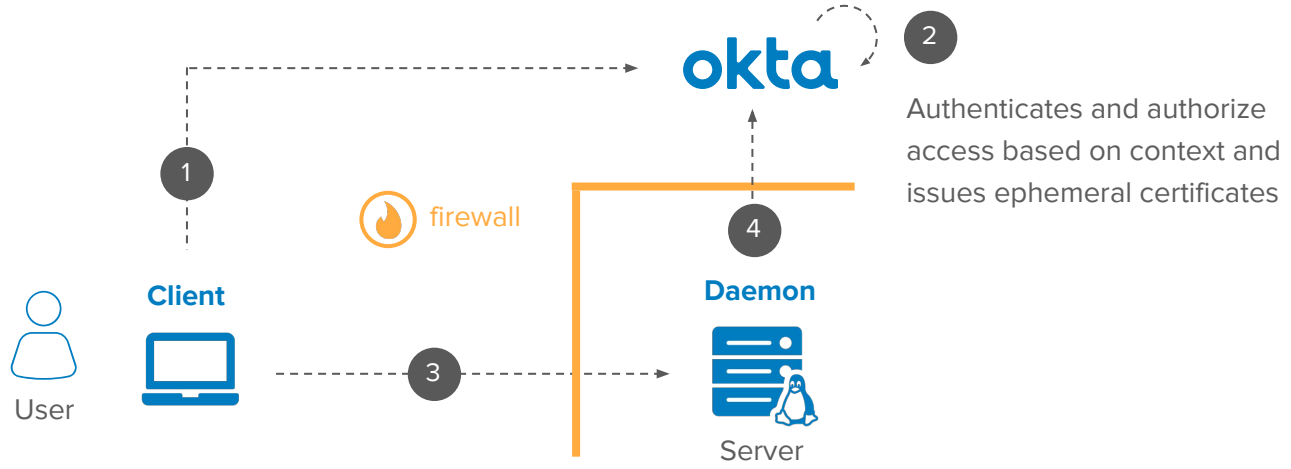



*PAM Module: Conceptual Diagram*

## Components

- **User**: Access a Linux or Unix Server via SSH.
- **Server**: Linux or Unix Server accessed by User.
- **Pluggable Authentication Module (PAM)**: Integrates natively with your Linux and Unix servers. During runtime, the PAM communicates with Okta to authenticate the user.
- **Okta**: Receives requests from the PAM Module to log in users with Multi-Factor Authentication.
- **Firewall**: The Linux server is usually available on the intranet and protected by a Firewall. The Okta integration uses only outbound connections and doesn't require firewall configuration for inbound requests. You can also use this integration to protect servers hosted in Cloud Providers.

## Advanced Server Access




*Advanced Server Access: SSH Conceptual Diagram*

## Components

- **User**: Access a Linux or Unix Server via SSH from a device with the server access client installed.
- **Server Access Client**: Communicates with Okta to establish ssh connections. In addition, re-evaluates the access context – user, device, server – during runtime to cut off access.
- **Okta**: Receives requests from the Server Access Client. Validates user, device, and server context and issues ephemeral certificates for authentication on servers. The certificates are bound to the user, device, and server and cannot be reused.
- **Server**: Linux or Unix Server accessed by User.
- **Daemon**: Server access daemon. Implements configuration on the server side to accept ephemeral certificates issued by Okta. In addition, it manages local users and group accounts, audits the operating system, and regularly re-evaluates the access context during runtime to cut off access.
- **Firewall**: Both the user and the Linux server can sit on the intranet. The server can also be hosted in cloud providers and protected by a Firewall.

## Use-Cases supported

### Authentication

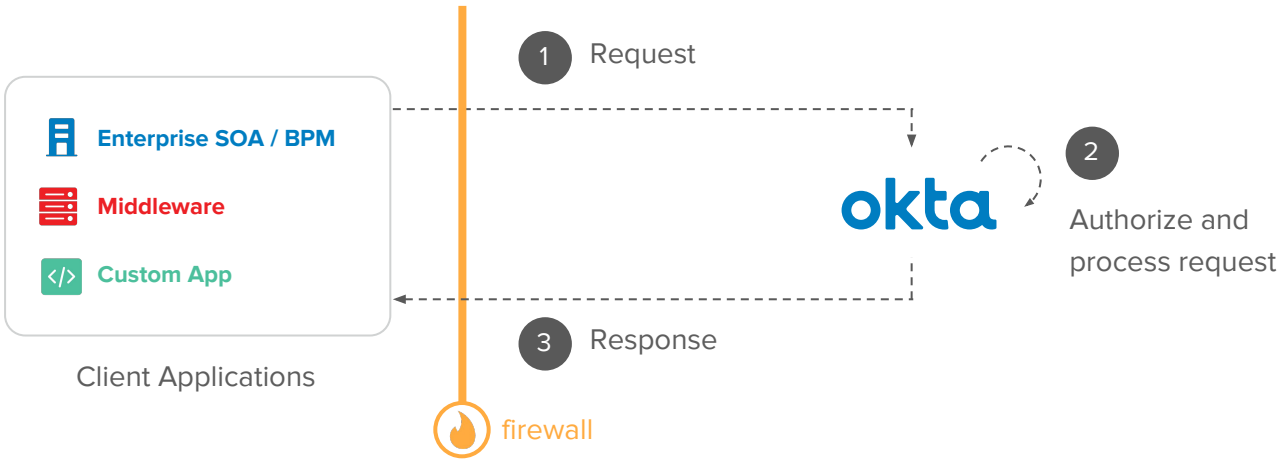
- Access Linux and Unix Servers with MFA provided by Okta
- Provides ephemeral client-certificate based authentication for Linux and Unix servers

# Okta Management APIs (REST APIs)

Okta provides native REST APIs that you can use for managing configurations, policies, and entities plus access system logs externally. The Okta APIs are used for automating the system configuration for integrating with 3rd party systems such as Identity Management, CASB, and Incident Response solutions. Okta offers a complete documentation and Postman collections developers can use to understand how the integration works and expedite the development and integration processes.

## Typically supported by

- Web Applications that support HTTP and the REST protocol
- API Gateways
- SOA and BPM solutions




*REST API: Conceptual Diagram*

## Components

- **Client Applications**: Perform REST API requests to Okta following the syntax defined by Okta.
- **Firewall**: The client application can be located on the intranet and protected by a Firewall, as long as it can make outbound connections to your Okta tenant (i.e., https://org.okta.com) via port 443.
- **Okta**: Validates and processes API requests and retrieves responses for the requester service.

## Use-Cases supported

### Read data from Okta

- Read Okta Users, Groups, and Apps.
- Read Okta System Configuration and Policies
- Access Reports and Logs externally

### Write data to Okta

- Manage Users, Groups, and Apps externally
- Manage System Configuration and Policies externally
- Automate Okta configuration

### Authentication

- Authenticate and MFA users in Okta

## References

Okta Developers Documentation Index

Okta API Design Principles

Postman Collections