Identity and Access Management for Hybrid Environments

KEY USE CASES

- SSO for non-SAML legacy or custom applications (e.g. Kerberos, NTLM, header-based).
- Secure external access to SharePoint portals.
- Multiple application access from a single portal.
- Directory chaining for secure on-premises user authentication.
- OAuth and OpenID Connect integration for secure delegation of app and API access.

Okta and F5 provide a solution to seamlessly manage access to all applications, on-premises and in the cloud. It helps extend the Okta IDaaS user experience and IT controls to on-premises, legacy, and custom applications.

Overview

With the rapid transition to SaaS, PaaS, and IaaS, enterprises often operate in IT environments that combine cloud environments with legacy applications on-premises. Enterprises are beginning to centralize IAM programs around IDaaS, moving the core of identity management to the cloud. With this transition comes the need to modernize on-premises applications or implement solutions with more direct integration to IDaaS.

F5® BIG-IP Access Policy Manager® (APM) can be deployed and configured with Okta, enabling IT administrators to manage secure access to on-premises applications, as well as those pre-integrated in the Okta platform.

No Application Left Behind

Using BIG-IP APM with Okta, end users can authenticate once into Okta and seamlessly access on-premises applications. BIG-IP APM helps extend the Okta authentication capability to applications that do not have native SAML authentication mechanisms or to those that require header-based, Kerberos, or NTLM authentication. BIG-IP APM also provides an additional layer of security for on-premises applications by securing all HTTP traffic to and from an application.

External Access to SharePoint

It can be challenging for external users, such as contractors or partners, to access SharePoint Server (on-premises). Okta can integrate with SharePoint for SSO via federation. However, certain SharePoint modules, such as SharePoint business intelligence features, require a Kerberos token.

BIG-IP APM enables the exchanging SAML assertions for Kerberos tokens, unlocking the full SharePoint functionality. Together, BIG-IP APM and Okta can enforce role-based access policies and context-based, multi-factor authentication.

One End User Portal for All Applications, On-Premises and in the Cloud

Typically, organizations using the Okta portal want all their end users' applications exposed and accessible through the portal. Integrating Okta with BIG-IP APM enables users to log in once to Okta to access all applications, both cloud-based and on-premises, in one place.

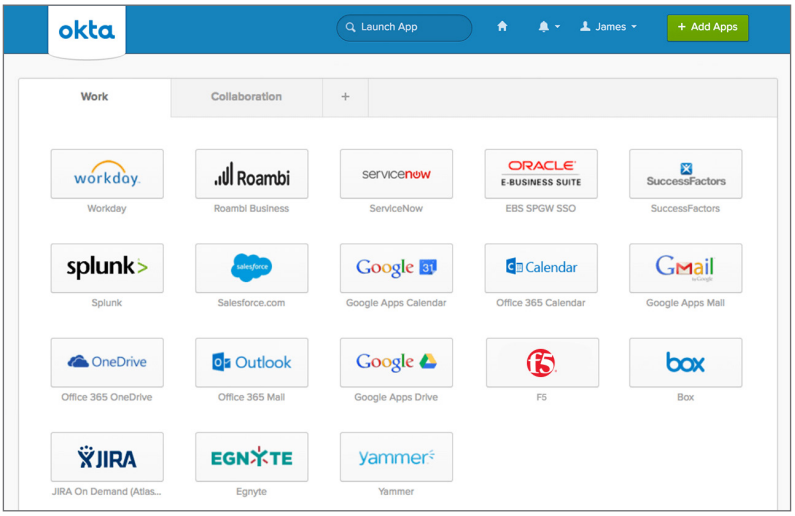

Figure 1: Okta web portal.

Keep Authentication On-Premises with Directory Chaining

The simplicity and security benefits of IDaaS are clear; however, having copies of the corporate directory in the cloud is not for everyone. For organizations that want to maintain corporate directory services on-premises, Okta and BIG-IP APM use directory chaining. Directory chaining enables Okta to transparently redirect authentication requests to BIG-IP APM on-premises. The end user has the same Okta experience without the need to maintain full directory information in the cloud.

Delegate Authentication and Authorization

BIG-IP APM and Okta work seamless together to support OAuth and OpenID Connect. This solution enables delegated authentication and authorization capabilities, where BIG-IP APM acts as a resource server in front of applications, while Okta acts as the authorization server. This configuration enables APIs, native apps, and mobile apps to have authentication and authorization functions delegated to a trusted party, eliminating the complexity and cost of implementing discrete systems.

Application Authentication Mechanism	Integration
Pre-built integration in Okta Application Network	Okta
Federation protocols (SAML, WS-Fed, OpenID Connect)	Okta
Log in form	Okta
No native authentication	Okta + BIG-IP APM
Kerberos/NTLM Exchange Authentication	Okta + BIG-IP APM
Header-based authentication	Okta + BIG-IP APM
Reverse proxy—access on-premises app from outside firewall	Okta + BIG-IP APM
Secure HTTP traffic to/from on-premises app	Okta + BIG-IP APM

To learn more about F5 security solutions, visit f5.com/security or email OktaQuestions@f5.com.

DC0318 | OV-SEC 211113605 | 0318