Identity and Access Management for Hybrid Environments

COMMON USE CASES

- Single sign-on (SSO) and multi-factor authentication (MFA) for all apps
- On-premises user authentication with directory chaining

Okta and F5 Networks provide secure access to all applications, on-premises and in the cloud, with a simple, fast single sign-on experience.

With the rapid transition to SaaS, PaaS, and IaaS, enterprises often operate in IT environments that combine cloud environments with legacy applications on-premises. To keep up with rapid the transformation to new cloud-delivered applications, organizations are centralizing identity around IDaaS, moving identity and access management (IAM) to the cloud. With this transition, businesses are challenged to integrate on-premises and legacy applications into cloud-based IAM solutions without too much disruption.

F5® BIG-IP® Access Policy Manager® (APM) can be deployed and integrated with Okta Identity Cloud. This enables IT administrators to manage secure access to not only the thousands of the applications in the Okta Integration Network, but also legacy (non-SAML) and on-premises applications as well.

See the table below to explore how F5 and Okta products work together so you can access your applications safely, regardless of environment.

Single sign-on (SSO) and multi-factor authentication (MFA) for all applications	F5 is the SAML Service Provider (SP)	Okta is the IDaaS and Identity Provider (IdP) via SAML v2.0
On-premises user authentication with directory chaining	F5 bridges the on-premises IdP for cloud-based authentication	Okta delivers the Okta SSO, portal, and user experience

Access Control for Every Application

Using F5 APM with Okta can authenticate end users once into Okta and seamlessly access any application regardless of where it resides, cloud-based or on-premises. F5 helps extend the Okta single sign-on and federation capabilities to applications that do not support modern authentication protocols, for example those that utilize header-based, Kerberos, or NTLM authentication.

Seamless Access to All Applications

Typically, organizations using the Okta Integration Network (OIN) App Catalog want all their end users' applications exposed and accessible through the portal. Integrating Okta with F5 enables users to log in once and access all applications, both cloud-based and on-premises, in one place.

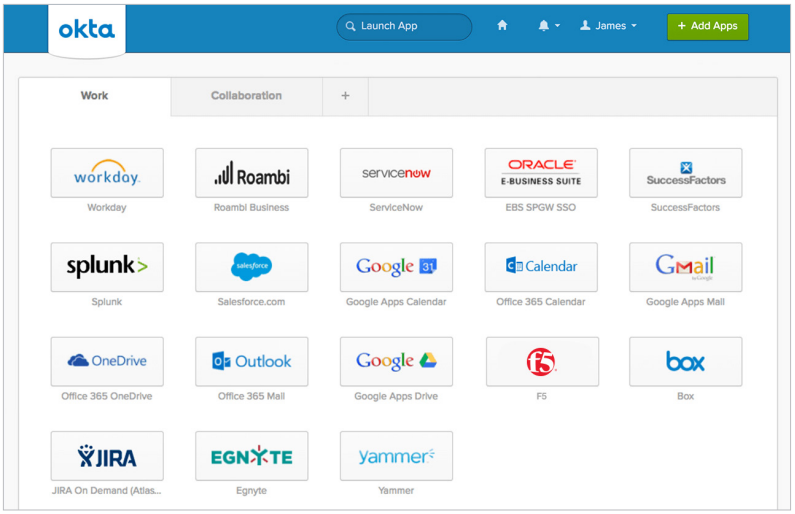

Figure 1: Okta Integration Network App Catalog

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

F5 and Okta work seamlessly together to support OAuth and OpenID Connect. This solution enables delegated authentication and authorization capabilities, where F5 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.

To learn more about F5 security solutions, visit f5.com/security or email f5_okta@f5.com. To find out more about Okta, please visit okta.com/f5.

DC0319 | OV-SEC 319043610 | 0319