F5 Access Manager

F5 Access Manager is a secure, flexible, high-performance access management proxy solution that provides unified global access controls for users, devices, and APIs.

Security Starts with Trusted Access

Trusted Access

Your apps are the gateway to sensitive data. The Access Manager proxy-based access controls enable a zero-trust model for both internal and external application access. Applications are protected while extending trusted access to users, devices, and APIs. With trusted access ensured, your business can expand beyond traditional security boundaries to unlock new business models and operational efficiencies—without sacrificing security or user experience.

Visual Policies

Access Manager simplifies the creation and implementation of sophisticated, context-based access policies. The Access Manager Visual Policy Editor enables you to rapidly design customized access policies with just about any access session variable available, including multi-factor authentication (MFA), context-based step-up authentication, and end-point security posture checks. In addition to enforcing access policy for unmanaged mobile devices, Access Manager also integrates with mobile device management solutions to enable expanded access policy enforcement capabilities for managed devices. Polices can be applied to individual applications or for specific functions within an application. Policy customization lets you apply access controls in proportion to the sensitivity of the application.

Accelerate Business Innovation

DevOps and NetOps

As IT transforms to cloud and mobile applications as the standard, Access Manager helps you adopt new business applications faster. As a centralized solution for access control, Access Manager can help you to accelerate deployment of new applications by offloading front end authentication from the application. DevOps can hand off applications to NetOps faster and NetOps delivers a consistent user experience that is more efficiently deployed and managed.

Single Sign-on and Federation

Access Manager integrates with existing single sign-on and identity federation, so your users can access all their business applications with a single login. New applications can be rapidly adopted by users, accelerating the time to value on new technology. Your existing application launchpad or the Access Manager dynamic Webtop gives users one-click access to the applications and resources they're authorized to access, based on their identity, context, and group membership.

Bridge to the Cloud

Cloud and SaaS applications have become the standard; however, many organizations can't move all applications off-premises. The result is a heterogenous environment that can be a challenge to integrate into cloud-based identity as a service (IDaaS) solutions. Access Manager bridges on-premises applications to the cloud. Integrations with Okta, Microsoft, VMware, and others enable existing on-premises applications to be accessible through IDaaS solutions, even if the applications are not SAML-enabled.

Streamline Access Management

Identity-Aware Proxy

Access Manager helps reduce access management cost and complexity. As an identity-aware proxy, it acts as a centralized front end for all business applications, protecting them from being directly accessed by bad actors. Centralization of access management can also help unify technology silos across the organization, including on-premises, cloud, and heterogenous application environments.

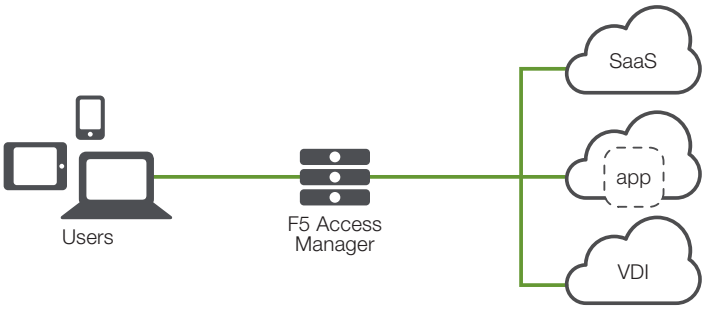

Figure 1: The Idendity Aware Access Proxy

OAuth and OpenID Connect

Access Manager supports OAuth 2.0 and OpenID Connect (OIDC) to enable access authorizations from trusted third-party identity providers such as Google, LinkedIn, Okta, Azure AD, and others. Access Manager serves as a resource server for both users and APIs, granting trusted access to protected resources after authorization is provided the by the third-party authorization server. This enables applications to use existing authentication services (e.g. Azure AD), simplifying the user experience and the burden of storing and maintaining additional user account and credential information.

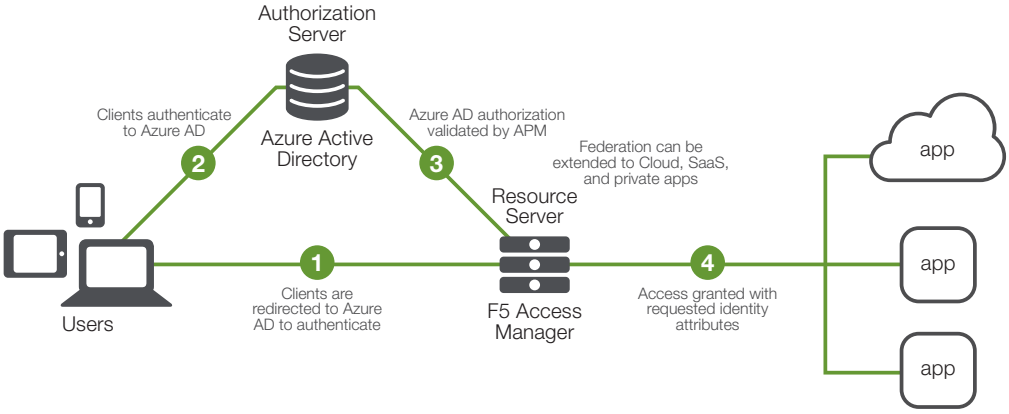

Figure 2: Application Access Control with OAuth

The Universal Translator

Access Manager serves as a translator, enabling SSO regardless of whether the application is SAML-enabled. When applications do not accept SAML, Access Manager policies and rules can convert the access request to the appropriate authentication for that application—header-based, Kerberos, or a non-standard alternative. This enables and integrates SSO for virtually any application.

To learn more, visit f5.com or contact sales@f5.com.

DC0718 | OV-SEC 249690710 | 0718