Access Policy Manager

F5's Access Policy Manager (APM) is a secure, flexible, and high-performance access management proxy solution. APM provides unified global access controls for users, devices, applications, and APIs.

Access Management

Identity-aware proxy

APM reduces access management cost and complexity. As an identity-aware proxy, it acts as a secure, centralized front end for all business applications, protecting them from direct access by bad actors. APM also enables protection for your applications through support for industry standards, including Secure Assertion Markup Language (SAML) and OpenID Connect (OIDC). Centralization of access management also helps unify technology silos across your organization, including on-premises, cloud, and other seemingly disparate application environments.

Single sign-on (SSO) and access federation

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

OAuth and OpenID Connect

Access Policy Manager supports OAuth 2.0 and OIDC, enabling social login, easing mobile application access and simplifying access authorization from trusted third-party identity providers like Google, LinkedIn, Okta, Azure AD, and others. APM serves as a resource server for both users and APIs, granting trusted access to protected resources after authorization is provided by the third-party authorization server. This lets apps use existing authentication services (e.g. Azure AD), simplifying the user experience and eliminating the burden of storing and maintaining additional user account and credential information.

A universal translator

APM serves as a translator, enabling SSO regardless of whether an application is SAML-enabled or not. When applications don't accept SAML, APM policies and rules can convert the access request to the appropriate authentication for that app—header-based, Kerberos, or a non-standard alternative. This enables and integrates SSO for virtually any application, simultaneously simplifying the user experience and enhancing security.

A bridge to the cloud

Cloud and Software-as-a-Service (SaaS) applications are now the standard; however, many organizations can't move all their applications off-premises, to the cloud. The result is a mixed environment that's challenging to integrate into your cloud-based Identity-as-a-Service (IDaaS) solutions. APM bridges on-premises applications and cloud-based identity. APM works with Okta, Microsoft, VMware, and other IDaaS and identity access management (IAM) providers, allowing users to access existing on-premises applications through IDaaS, even if the apps aren't SAML-enabled.

Unified, Trusted Access

Trusted access

Your applications are the gateway to sensitive data. APM's proxy-based access controls deliver a zero-trust platform for internal and external application access. That means 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.

Unified global access

APM provides end-to-end security across your global infrastructure and beyond. Through user, application, network/cloud, and threat/vulnerability context-based policies, APM delivers:

- Secure remote and mobile access to applications, networks, and clouds via SSL VPN.
- A Datagram Transport Layer Security (DTLS) mode for remote connections, which secures and tunnels delay-sensitive applications.
- IPsec encryption for traffic between branch offices or data centers.
- Per-app VPN via an application tunnel, enabling access to a specific application without the security risk of opening a full network access tunnel.
- Per-app VPN access from mobile devices managed by leading enterprise mobility management (EMM) solutions, including VMware Horizon ONE (AirWatch) and IBM MaaS360—without user intervention.

APM also offers simple, broad virtual application and desktop support. It serves as a gateway for virtual application environments and includes:

- Native support for Microsoft Remote Desktop Protocol (RDP).
- Native secure web proxy support for Citrix XenApp and XenDesktop.
- Security proxy access for VMware Horizon.

Administrators can control the delivery and security components of enterprise virtualization solutions through APM's unified access, security, and policy management. The scalable, high-performance capabilities of APM also simplify user access and control in hosted virtual desktop environments.

Visual policies

Access Policy Manager makes it easier to create and implement sophisticated, context-based access policies. It includes a Visual Policy Editor (VPE), enabling you to rapidly design and update access policies with just about any access session variable available, including multi-factor authentication (MFA), context-based step-up authentication, and endpoint security posture checks. In addition to enforcing access policy for unmanaged mobile devices, APM also integrates with enterprise mobility management (EMM) solutions to extend access policy enforcement capabilities to managed devices. Policies can be applied per application or for specific functions within an application. Policy customization lets you apply access controls based on the sensitivity of the app.

Optional credential protection

User credentials need to be protected at all times because, unfortunately, all it takes is for an attacker to steal your credentials once to gain unfettered access to your network, cloud, devices, and apps. APM's optional add-on credential protection secures credentials from theft and reuse. It protects against Man-in-the-Browser (MitB) attacks with real-time, adaptable login encryption and obfuscation of user credential field names entered into its login page. APM renders credentials unreadable and unusable, even in the unlikely event an attacker successfully steals them. It also ensures login security for all apps associated via federation.

Accelerate Business Innovation

Enhancing DevOps and NetOps

As your company transitions to cloud and mobile applications as the standard, APM provides a centralized access control solution, helping you adopt new business apps faster. APM helps you deploy new applications faster by offloading front-end authentication from the application. As a result, your DevOps team can hand off applications to NetOps faster, enabling a consistent user experience that's more efficiently deployed and managed.

Protecting APIs

Today's modern application architecture uses a number of application programming interfaces (APIs). And attackers are now exploiting APIs to launch a myriad of attacks. Many organizations expose APIs to the public and their supply chain partners, leaving them vulnerable to exploitation. Also, many APIs are inadvertently left unprotected, again leaving them open to exploit. Organizations can ensure API security via authentication, especially if it's adaptable and protected by consistent, flexible authentication and authorization policies. APM enables secure authentication for REST APIs. It also makes sure appropriate authorization actions are taken. APM can integrate OpenAPI or "swagger" files, saving development time, resources, and cost, while establishing accurate API protection policies.