International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

# F5 APM Module: Centralized IAM and SSO

**Satish Yerram**

yerramsathish1@gmail.com

**Abstract**

**F5 Access Policy Manager (APM) brings identity and access management (IAM) and single sign-on (SSO) into the BIG-IP platform, helping organizations simplify secure access without juggling multiple tools or vendors. Acting as a centralized authentication proxy, APM supports modern standards like SAML, OAuth2, and OpenID Connect (OIDC), while also offering flexible customization through its Visual Policy Editor and iRules. Beyond basic federation, it provides zero-trust access enforcement, per-application VPN tunnels, endpoint posture validation, and hybrid integration for both cloud and on-premises environments. The advantage of APM is that it sits inline with application traffic, allowing it to apply policies in real time and inject user attributes directly into requests before they reach the app. In this paper, I will walk through the challenges of not having centralized IAM, explain the benefits of APM, share results from practical testing, and highlight its role in improving both security and user experience [1]–[5].**

**Keywords: Access Policy Manager, Single Sign On, IAM, SSO, Identity Access Management, F5 APM, SAML, OIDC, OAuth.**

## 1. Introduction

Enterprises today are managing a mix of traditional on-prem systems, SaaS applications, and multi-cloud workloads. Each environment brings its own identity challenges, and without a central solution, organizations often end up stitching together different tools, which creates more complexity than it solves. F5 APM simplifies this by integrating IAM and SSO into BIG-IP, the same traffic management system already trusted for load balancing and security. With APM, authentication flows do not happen somewhere else they happen directly in the traffic path. This means policies are enforced in real time, and applications can rely on identity attributes without having to manage federation protocols themselves. APM supports all the major standards like SAML, OAuth2, and OIDC, and it gives admins two powerful ways to build policies: a Visual Policy Editor for drag-and-drop simplicity, and iRules for advanced, programmable logic [1], [2].

## 2. Challenges Without Centralized IAM/SSO

When IAM and SSO are not centralized, organizations quickly run into operational and security headaches. Every new app might require its own custom integration with an identity provider, and in many cases, different teams end up solving the same problem multiple times. This leads to wasted effort, inconsistent authentication experiences, and security policies that vary from one system to another. Auditing becomes messy because identity logs are spread out across multiple apps and services, making it harder to prove compliance or detect suspicious activity. In multi-cloud setups, where apps may rely on different providers like Azure AD, Okta, or LDAP, the problem multiplies. Updating security flows becomes slow because logic is often baked directly into apps, meaning any policy change requires a development cycle. These gaps not only slow down the business but also open doors for attackers who thrive on inconsistency and weak identity practices.

## 3. Benefits of F5 APM

F5 APM addresses these issues by consolidating access control into a single, programmable layer. It natively integrates with identity providers like Azure AD, Okta, and LDAP directories, giving organizations flexibility to support both modern and legacy systems [1], [3], [4]. Instead of forcing apps to handle federation protocols, APM does the heavy lifting and passes identity details downstream in simple headers or cookies. This means apps get the information they need without being burdened with identity logic. Policies can be customized using the Visual Policy Editor for easy deployment, or with iRules when more advanced, context-aware access is needed [2]. APM also strengthens security by adding MFA, centralized session management, and detailed logging, all in one place. With policies that adapt dynamically to risk level, device posture, or location, APM helps organizations move toward a zero-trust security model without slowing down the user experience.

## 4. Methodology

For testing, APM was deployed as a reverse proxy in front of several enterprise applications that each used a different identity backend, including Azure AD, Okta, and on-prem LDAP directories. In this setup, APM acted as a SAML service provider, handling the authentication exchanges with the identity systems. Once users were authenticated, APM injected identity attributes like usernames, groups, and email addresses into headers, so applications could make role-based decisions without handling federation themselves. Policies were built to enforce access by role and to trigger step-up MFA for sensitive apps or high-risk scenarios, such as logins from unfamiliar locations. Logging and analytics features in APM captured performance metrics like authentication times, as well as detailed security events, which gave a clear view of how policies were being applied. This method showed not just how APM integrated with different providers, but also how it performed in real-world traffic scenarios.

## 5. Results

The evaluation confirmed that APM delivered smooth, seamless SSO across apps tied to different identity providers [1], [2], [3], [4]. Users were able to move between apps without repeated logins, and backend applications received the identity attributes they needed directly from APM. Policies successfully adapted to factors like device type and location, showing the value of context-aware controls. Branding and customizing login pages were simple, which made it easier to maintain a consistent enterprise look and feel. Importantly, performance remained strong. Authentication and inspection added very little overhead, even when handling large numbers of concurrent sessions. These results reinforced the idea that APM can sit inline without becoming a bottleneck, which is crucial for enterprises with heavy traffic demands.

## 6. Discussion

One of the biggest advantages of APM is its position in the traffic path. Because it's inline, it doesn't just broker identities — it actively enforces policies as requests flow through. That means it can inject headers with usernames, roles, or custom claims into traffic before it reaches the app, so applications don't need to manage federation themselves. This cuts down on development work, reduces complexity, and makes policies easier to manage across the entire environment. By consolidating these decisions into a single layer, organizations avoid the sprawl of third-party identity brokers and improve visibility into who's accessing what. Since APM can connect to both modern providers like Azure AD and Okta as well as traditional LDAP directories, it's a flexible option for companies that are running hybrid infrastructures [1], [2], [3], [4].

## 7. Core Capabilities of F5 APM

APM comes packed with features that cover both everyday IAM needs and advanced enterprise requirements [1]. It delivers zero-trust access by checking context for every request, supports identity federation with SAML, OAuth2, and OIDC, and integrates MFA methods like FIDO U2F, RADIUS, and push-based verification [3], [4]. It can connect with external providers like Google or LinkedIn, perform device posture checks using F5 Access Guard, and support per-app VPN tunnels for secure, scoped access. Administrators get a powerful Visual Policy Editor to build policies quickly, while advanced teams can use REST APIs or iRules for complex integrations. APM also scales well, with the ability to support hundreds of thousands of concurrent sessions per device. These capabilities make it not just an IAM tool, but a full platform for secure, context-aware access across cloud, SaaS, and on-prem systems.

## 8. Network Security

On the network side, APM improves security by controlling how traffic flows through VPNs [1]. Organizations can choose between full tunneling, where all traffic goes through the VPN for centralized enforcement, or split tunneling, where only corporate traffic is routed while other traffic flows normally. While split tunneling can boost performance, it also carries risks like malware bypassing corporate filters. To mitigate those risks, APM adds protections such as DNS relay proxies, enforcement of routing rules, and IP filtering to block non-corporate traffic. Access control lists (ACLs) provide another layer of defense, ensuring users only reach the resources they need. These ACLs can be predefined or pulled dynamically from identity systems like Active Directory, making policies more adaptive. Together, these controls strengthen the overall network security posture while still allowing flexibility for performance needs.

## 9. Session Management

Sessions are a common attack target, and APM includes a full set of controls to protect them [1]. It scopes sessions to specific profiles or servers, rotates session IDs to block fixation attacks, and allows admins to set limits on how many sessions a user can have at once. Session timeouts can be enforced based on inactivity or maximum length, and once sessions end, any sensitive data tied to them is immediately destroyed. APM encrypts session data like credentials with per-session AES-128 keys, making it extremely difficult for attackers to exploit stolen tokens. It also includes protections against denial-of-service by limiting concurrent sessions per IP and stopping brute-force attempts with CAPTCHAs, lockouts, and progressive delays.

In addition to these controls, APM manages authentication states through cookies that are set and validated during the login process. When a user first authenticates, APM creates the **MRHSession** cookie, which stores the session ID that ties the client browser to the server-side session object. Alongside it, the **LastMRH_Session** cookie may also be issued to help track the most recent session and improve reconnections. These cookies are typically marked with Secure and HTTPOnly flags to prevent exposure through client-side scripts and are bound to the client's IP when session binding is enabled. During authentication, the cookies are exchanged between the browser and APM with each HTTP request and response, allowing APM to validate the session before granting access to protected resources. If the session is terminated or times out, the MRHSession cookie is invalidated immediately, preventing replay attacks. This cookie-driven approach ensures that session management is tightly integrated with BIG-IP's policy engine, keeping the user experience smooth while maintaining strict security boundaries.

**10. Integrating F5 APM with On-Premises IAM (Example Ping Identity)**

APM works smoothly with on-prem IAM systems like Ping Identity, making it useful for hybrid environments. When deployed as a service provider, APM can pass authentication to Ping Identity while still enforcing its own checks like MFA and device posture validation. This adds a second layer of protection without complicating the user flow. APM can also act as an identity provider itself, handling logins and then passing user details like groups or roles to Ping or other applications. This flexibility means organizations don't have to rewrite applications or duplicate integration work. Instead, they centralize access decisions at the network edge, while still keeping their existing IAM tools in place. For companies balancing legacy systems with new cloud platforms, this hybrid approach helps ease the transition while keeping security consistent.

**11. Conclusion**

F5 APM brings IAM and SSO together in one place, right where application traffic flows. By unifying identity enforcement into BIG-IP, organizations can simplify integrations, improve visibility, and enforce zero-trust principles without slowing down the business. With features like policy-based access control, MFA, secure session management, and hybrid IAM support, APM is more than just a single sign-on tool — it's a complete platform for secure access. For enterprises dealing with complex, multi-cloud, and hybrid environments, APM offers a practical way to strengthen security while keeping performance and the user experience front and center.

**REFERENCES:**

[1] F5 Networks. (2023). *Access Policy Manager Overview*. https://www.f5.com/products/access-policy-manager
[2] F5 DevCentral. (2022). *Writing iRules for Access Control*. https://devcentral.f5.com/
[3] Microsoft. (2023). *Integrating Azure AD with SAML*. https://learn.microsoft.com/
[4] Okta Docs. (2023). *OAuth and OpenID Connect Support*. https://developer.okta.com/
[5] Gartner IAM Report. (2022). *IAM Trends and Tools Comparison*. https://www.gartner.com/