



BIG-IP ACCESS POLICY MANAGER

WHAT'S INSIDE

- 2 Simplify Access
- 4 Unify Access
- 6 Streamline Virtual Application Access
- 8 Centralize Dynamic Access Control
- 11 API and Credential Protection
- 11 Enhance Visibility and Reporting
- 13 Unparalleled Flexibility, High Performance, and Scalability
- 15 BIG-IP APM Features
- 17 F5 BIG-IP Platforms
- 17 F5 Global Services
- 17 More Information

CONNECT TO THE EXTENDED ENTERPRISE WITH CONFIDENCE AND SECURITY

Applications are the gateways to your critical and sensitive data. And, today, your apps can be hosted anywhere – on premises, co-located, or in a public or private cloud. Secure access to your applications continues to be a necessity. But ensuring that your users have secure, authenticated access anytime, anywhere, to only the applications that they are authorized to access is becoming difficult to maintain. There are different methods of application access with which to deal. There are various means of ensuring authorized user identity, as well as different methods of single sign-on (SSO) and federation, all in an attempt to simplify the user access experience.

With digital transformation touching every part of today's enterprise, cloud and SaaS applications are becoming the new enterprise application standard. Many organizations, however, find that they are unable to migrate all of their applications off premises. In addition, many enterprises are unable or unwilling to migrate all of their apps to the cloud at the same time. These situations result in applications being hosted in a variety of locations, with differing and many times disparate authentication and authorization methods, which can't work seamlessly across your existing SSO or identity federation means, including Identity-as-a-Service (IDaaS).

F5® BIG-IP® Access Policy Manager® (APM) is a secure, flexible, high-performance access management proxy solution that delivers unified global access control for your users, devices, applications, and application programming interfaces (APIs). Through its single management interface, BIG-IP APM converges and consolidates remote, mobile, network, virtual desktops, and web access. With BIG-IP APM, you can create and enforce simple, dynamic, intelligent access policies.

KEY BENEFITS

- **Simplify access**

Bridge access to both on-premises and cloud apps with a single login via SSO even for applications not enabled for Security Assertion Markup Language (SAML).

- **Unify control**

Consolidate management of remote, mobile, network, virtual, and web access in one control interface with adaptive identity federation, SSO, and multi-factor authentication (MFA).

- **Reduce costs**

Replace web access proxy tiers with an integrated solution for VMware Horizon/Workspace ONE, Microsoft Office365, Citrix XenApp, Microsoft Exchange, and others, and provide a secure proxy for Microsoft Active Directory Federation Services (AD FS).

- **Secure web access**

Control access to web-based applications and web content, while defending against highly complex web threats.

- **Centralize and manage access control**

Simplify and secure access management to your network, clouds, and applications via dynamically enforced, context-based policies for users, applications, networks/clouds, and threats/vulnerabilities.

SIMPLIFY ACCESS

BIG-IP APM combines centralized network access control, federated identity, SSO, and adaptive authentication into a single flexible, scalable application delivery solution, simplifying and consolidating your access infrastructure.

Identity federation and SSO

SAML-based authentication reduces user dependency on passwords, increasing security and improving both user experience and productivity.

SAML 2.0 further enhances BIG-IP APM identity federation and SSO options by supporting connections initiated by both SAML identity providers and service providers. This functionality extends identity federation and SSO capabilities to cloud-based applications and enables identity federation across an organization's BIG-IP products. It empowers administrators to centrally disable user authorized access to any identity-enabled applications, regardless of where they reside, saving time and boosting administrative productivity.

Additionally, BIG-IP APM serves as an SSO translator, enabling SSO via SAML to applications that support SAML, as well as to those that do not. For applications that don't, BIG-IP APM converts authentication access to the appropriate authentication standard supported by the application. This ensures users can utilize SSO to access applications—regardless of their location (i.e., on-premises or in the cloud) or whether or not the apps support SAML.

BIG-IP APM secures the transport and reduces the flow of SAML messages through browsers using SAML artifact binding. This addresses certain browser restrictions and extends identity federation and SSO support to automatically submitted forms that do not support JavaScript. This solution extends identity federation to client-based applications and other browser-less environments—including desktop applications and server code in web apps—and streamlines user workflow by supporting SAML Enhanced Client or Proxy (ECP) profiles.

BIG-IP APM works with the OAuth 2.0 open-standard for authorization. It can serve as a client for social networking logins, as an authorization delegate for SaaS applications, and can enhance protection for and authorization of APIs for web services.

With support for SSO and Kerberos ticketing across multiple domains, BIG-IP APM enables additional types of authentication, such as U.S. Federal Government Common Access Cards and the use of Active Directory authentication for all applications. Users are automatically signed on to back-end applications and services that are part of a Kerberos realm. This provides a seamless authentication flow once a user has been authenticated through a supported user-authentication mechanism. BIG-IP APM also supports smart cards with credential providers, so users can connect their devices to their network before signing in.

KEY BENEFITS (CONT.)

- **Defend your weakest links**
Protect against data loss, malware, and rogue device access with comprehensive endpoint posture and security checks.
- **Protect APIs**
Enable secure authentication for REST and SOAP APIs and integrate OpenAPI or “swagger” files to ensure appropriate authentication actions while saving time and cost.
- **Do it all at scale**
Support all users easily, quickly, and cost-effectively with no performance trade-offs for security, even in the most demanding environments.

Address hybrid Office 365 deployments

BIG-IP APM delivers secure identity federation and SSO for hybrid deployments. For instance, if you have deployed Office 365 and maintain Exchange mailboxes on premises, BIG-IP APM provides a seamless user experience by enabling SSO to Office 365 as well as to on-premises email, while ensuring appropriate authentication. If you have deployed Office 365, migrated your email, and have chosen to use Microsoft Azure Active Directory for authentication, BIG-IP APM can proxy ActiveSync and encrypt user credentials before sending them to Office 365, delivering additional security for your most important user data. Integration with leading mobile device management (MDM) and enterprise mobility management (EMM) solutions helps policies to be consistently applied to mobile access, too.

Automatically synchronize Exchange services

With BIG-IP APM, you can synchronize email, calendar, and contacts with Microsoft Exchange on mobile devices that use the Microsoft ActiveSync protocol. By eliminating the need for an extra tier of authentication gateways to accept Microsoft Outlook Web Access, ActiveSync, and Outlook Anywhere connections, BIG-IP APM helps consolidate infrastructure and maintain user productivity. When migrating to Exchange 2010, this solution works with Active Directory to facilitate seamless mailbox migration over time. When migration is complete, BIG-IP APM provides managed access to Exchange with single URL access—regardless of the user, device, or network.

Adaptive authentication and infrastructure consolidation

BIG-IP APM provides you with seamless user access to web applications in a highly available and heterogeneous environment, which in turn improves business continuity and boosts user productivity for your organization. It supports and integrates with AAA servers and user credential stores—including Active Directory, Lightweight Directory Access Protocols, RADIUS, and Native RSA SecurID—to deliver high availability through the intelligent traffic management capabilities of BIG-IP® Local Traffic Manager™ (LTM). In addition, BIG-IP APM recognizes when an RSA SecurID software token is installed on a user's Windows or Mac device, prompting the user for an RSA PIN, seamlessly authenticating them. It also supports Google reCAPTCHA V2 for authentication and contextual authentication.

To help you deploy MFA, BIG-IP APM includes one-time password authentication via email or SMS. Through F5's extensive partner ecosystem, it also integrates with most leading MFA solutions, including Identity-as-a-Service (IDaaS) offerings, like Okta and others. By integrating with your existing MFA solution, BIG-IP APM enables adaptive authentication, allowing various forms of single-, two-, or multi-factor authentication to be employed based on user identity, context, and application access.

To enforce step-up authentication, you can insert a stronger form of authentication or revalidate authentication per request within an access session—for example, when a user attempts to access additional sensitive web URIs or extend an existing session. BIG-IP APM supports step-up authentication for single- and multi-factor authentication. Any session variable may be used to trigger step-up authentication, and you can utilize additional authentication capabilities or select from a number of our partner offerings. In addition, any session variable may be part of access policy branching (such as URL branching) per request policy.

Many authentication solutions use application coding, separate web server agents, or specialized proxies that present significant management, cost, and scalability issues. With AAA control, BIG-IP APM enables you to apply customized access policies across many applications and gain centralized visibility of your authorization environment. You can consolidate your AAA infrastructure, eliminate redundant tiers, and simplify management to reduce capital and operating expenses.

Intelligent integration with identity and access management

F5 partners with leading on-premises and cloud-based identity and access management (IAM) vendors, such as Okta, VMware, and Ping Identity. This integration enables local and remote user SSO via SAML to applications based on premises or in a data center. For organizations that do not wish to replicate their user credential store in the cloud with IDaaS or cloud-based IAM offerings, BIG-IP APM works with F5's IAM vendor partners to help these organizations maintain control of on-premises user credentials. This is accomplished by creating a bridge between the IAM vendor's offering and the local authentication services. This bridge, or identity provider chain, leverages SAML to federate the user identity.

UNIFY ACCESS

Today's workforce is mobile, with users demanding access to applications—anywhere, from any device, and often over unsecured networks. Ensuring always-connected users have fast and secure access to applications, whether on premises or in the cloud, remains a challenge for many organizations. By implementing policy-based access decisions, BIG-IP APM strengthens corporate compliance with security standards, corporate controls, and industry and government regulations.

A single solution for all access

BIG-IP APM is positioned between your applications and your users, providing a strategic application access control point. It protects your public-facing applications by providing granular policy for identity- and context-aware external user access, while consolidating your access infrastructure. It secures remote and mobile access to your corporate resources from all networks and devices. BIG-IP APM converges and consolidates all access—network, cloud, and application—within a single management interface. It also enables and simplifies the creation of dynamic access policies that are easy to manage.

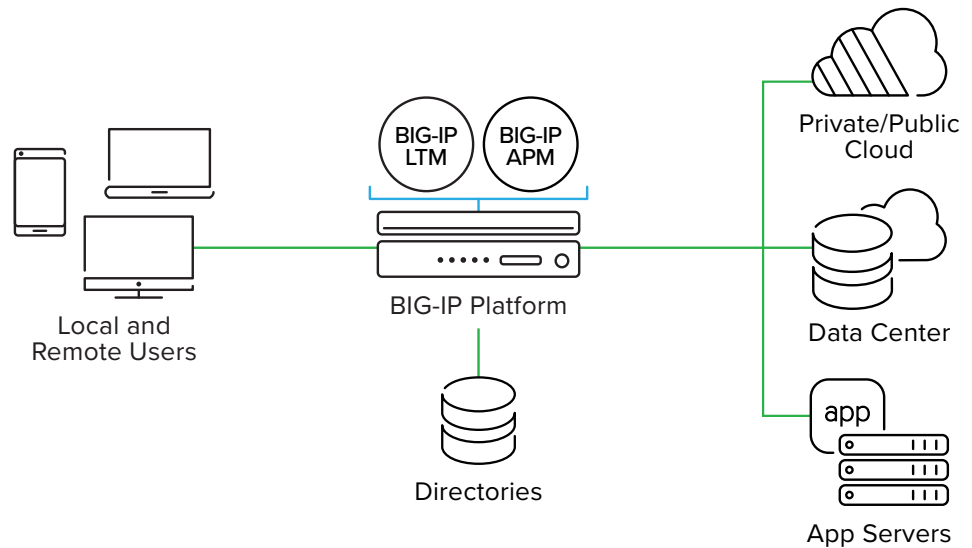


Figure 1: BIG-IP APM consolidates and manages access to all applications, networks, and clouds.

“Always connected” access

F5 provides users with secure access to applications, networks, and clouds from computing devices via the BIG-IP Edge Client and F5 Access, an optional mobile client for ensuring secure access from mobile devices.

The BIG-IP Edge Client delivers secure access via Secure Socket Layer (SSL) virtual private network (VPN) for today’s remote and mobile workforce, available for Apple MacOS and iOS, Microsoft Windows, Linux platforms, Google Android, and Chromebook. For remote connections, it offers a Datagram Transport Layer Security (DTLS) mode, which secures and tunnels applications that are delay sensitive. For traffic between branch offices or data centers, IPsec encryption is enabled. BIG-IP APM automatically detects domains and reconnects after losing a VPN connection or can automatically disconnect when a LAN connection is detected. You can also enable users to use their Microsoft Windows operating system login to establish an always-on VPN tunnel via the BIG-IP APM on Windows.

When deployed with leading MDM and EMM offerings, BIG-IP APM augments their mobile and remote access gateway support—increasing access scalability, consolidating access gateways, and decreasing access infrastructure for enterprises deploying those solutions. BIG-IP APM also enables per-app VPN access from mobile devices managed by VMware Horizon ONE (AirWatch), IBM MaaS360, and other MDM and EMM solutions—without requiring user intervention.

Robust endpoint security

BIG-IP APM inspects and assesses users' endpoint devices, examining their security posture and determining if the device is part of the corporate domain. Based on the results, BIG-IP APM will apply dynamic access control lists (ACLs) to deploy context-based user, application, network/cloud, and threat/vulnerability security. BIG-IP APM includes preconfigured, integrated endpoint inspection checks, including checks for OS type, antivirus software, firewall, file, process, registry value validation and comparison (Windows only), as well as device MAC address, CPU ID, and HDD ID. For mobile devices running iOS or Android, BIG-IP APM's endpoint inspection checks the mobile device UDID and jailbroken or rooted status.

The BIG-IP Edge Client and F5 Access integrate with leading MDM and EMM solutions—including VMware Horizon ONE (AirWatch) and IBM MaaS360—to perform device security and integrity checks. Context-aware policies are assigned based on the device's security state. These policies enable, modify, or disable application, network, and cloud access from a user's device. Administrators may map hardware attributes to a user's role to enable additional decision points for access control. A browser cache cleaner automatically removes any sensitive data at the end of a user's session.

Secure application tunnels

If an endpoint doesn't comply with your defined security posture policy, an application tunnel can provide access to a specific application without the security risk of opening a full network access tunnel. For example, users may simply click their Microsoft Outlook clients to get secure access to their email, from anywhere in the world. Application tunnels are also WAN optimized to more efficiently deliver content to users.

STREAMLINE VIRTUAL APPLICATION ACCESS

Virtual desktop and application deployments must scale to meet the needs of thousands of users and hundreds of connections per second. BIG-IP APM serves as a gateway for virtual application environments. It includes native support for Microsoft Remote Desktop Protocol (RDP), native secure web proxy support for Citrix XenApp and XenDesktop, and security proxy access for VMware Horizon. Administrators gain control over the delivery and security components of enterprise virtualization solutions via BIG-IP APM's unified access, security, and policy management. These scalable, high-performance capabilities simplify user access and control in hosted virtual desktop environments. BIG-IP APM delivers simple, broad virtual application and desktop support.

Simplify VMware virtual application access

BIG-IP APM provides a single, scalable solution for remote and local network access policy and control. The solution can be extended to other applications, providing a simple, low-cost, highly scalable enterprise infrastructure. BIG-IP APM supports the latest versions of VMware Horizon, ensuring maximum performance, availability, and scalability for VMware End User Computing (EUC) implementations.

Enterprises may use SSO from smartcards with BIG-IP APM and VMware View Connection Server, consolidating gateways and cost for VMware EUC deployments. BIG-IP APM supports two-factor authentication via RSA SecureID and RADIUS through the native client for VMware EUC deployments. On-demand validation is available for mobile clients, as well as zero clients.

BIG-IP APM enables single SSO to VMware Identity Manager (vIDM), enforcing authentication and access policies. SSO is enabled via WebSSO and native VMware Horizon client support using PCoIP and Blast Extreme. The native client is launched from vIDM and establishes proxy connections through BIG-IP APM. Citrix ICA Proxy is also supported, allowing BIG-IP APM to publish Citrix apps to the VMware vIDM portal. This solution also delivers data loss protection by controlling USB redirection and client-drive mapping for VMware Horizon desktops via context-based policies.

Streamline Microsoft RDP access

BIG-IP APM, when integrated with the Microsoft RDP protocol, enables the remote desktop access needed to install client-side components or run Java. It allows Microsoft RDP to be available for use on new platforms, such as Apple iOS and Google Android devices. It also enables native RDP clients on non-Windows platforms such as Mac OS and Linux, where previously only a Java-based client was supported.

The Microsoft RDP native client can also be launched directly from BIG-IP APM dynamic Webtop. Webtop shows only the applications authorized for and available to a user based on their identity and context—regardless of if the applications are on-premises or in the cloud. BIG-IP APM's Microsoft RDP support works with any Microsoft, Apple, Google web browser, or RDP app installed.

Consolidate Citrix infrastructure

BIG-IP APM supports Citrix XenApp and XenDesktop simultaneously, as well as Citrix StoreFront, further consolidating support for Citrix desktop and application virtualization infrastructure. For instance, in a typical Citrix XenApp or XenDesktop implementation, an administrator can save significant cost by replacing Citrix authentication management, Secure Ticket Authority (STA), NetScaler, and XenApp Services sites (required for Citrix sourced enterprise deployment) with BIG-IP APM.

Flexible remote desktop access

As web browser plug-ins become more difficult to support due to rapid changes, lockout, and abandonment of specific plug-in technologies, BIG-IP APM continues to enable simple remote desktop protocol (RDP) that adapts to your organization's deployment and user experience requirements.

While ActiveX- and Java-based plug-ins are disappearing or left unsupported by web browsers, native Java RDP applications must update or they risk being incompatible. In addition, support for device- or operating system-specific RDP remote access clients is labor-intensive and time-consuming. To address these challenges, BIG-IP APM supports client-less, browser-based RDP access. It serves as the single point of administration, while enabling universal remote access from any browser, without installation or clients.

BIG-IP APM supports a Java-based, platform-independent RDP client. The client is dynamically downloadable from BIG-IP APM with support for SSO, the ability to support up to sixteen parallel monitors, and with no administration rights required on endpoint devices.

CENTRALIZE DYNAMIC ACCESS CONTROL

By enabling the creation and enforcement of user, application, network/cloud, and threat/vulnerability context-based dynamic access decisions, BIG-IP APM strengthens corporate compliance with security standards—and industry and government regulations—while ensuring users stay productive with appropriate, authenticated, secure application access.

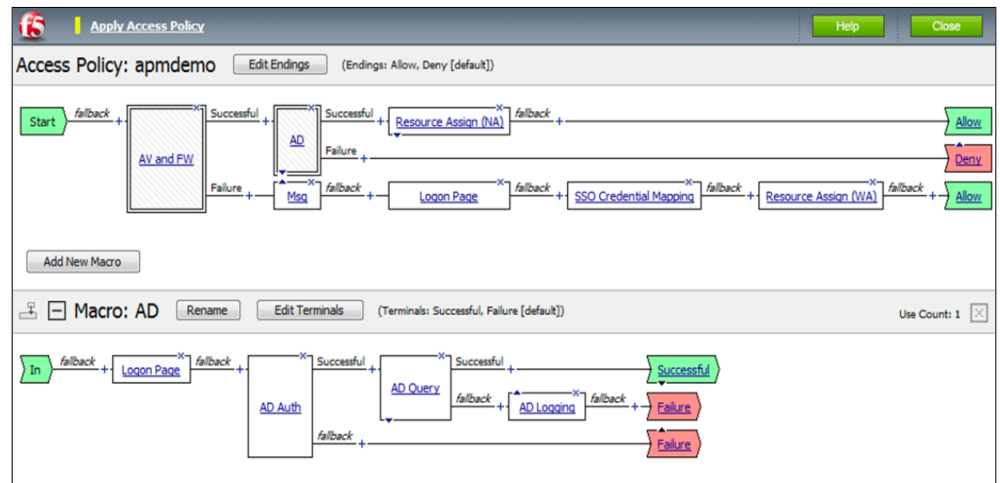
Advanced Visual Policy Editor

Through its advanced graphical Visual Policy Editor (VPE), BIG-IP APM makes designing and managing granular access control policies on an individual or group basis fast and simple. With VPE, you can efficiently create and edit entire dynamic access policies in just a few clicks.

For example, you can design an authentication server policy integrated with RADIUS, and then either assign resources for access once authorization is complete or deny access for failure to comply with policy. A geolocation agent provides automatic lookup and logging. This simplifies the configuration process and helps you customize user access rules according to your organization's geolocation policy.

BIG-IP APM's VPE can define rules per URL path. For example, policies can restrict application, network, and cloud access based on IP address. These restrictions can also be based on context-based attributes such as a specific day, time of day, or other user, application, network/cloud, and vulnerability. By centralizing and simplifying the management of contextual policies, you can efficiently manage fine-grained user access to applications, networks, and clouds.

Figure 2: The BIG-IP APM advanced VPE makes it fast and easy to create, modify, and manage granular application-, user-, network/cloud, and vulnerability context-based access policies.



Dynamic access control

BIG-IP APM enforces access authentication using ACLs and authorizes users with dynamically applied layer 4 and layer 7 ACLs on a session. Both L4 and L7 ACLs are supported based on endpoint posture as a policy enforcement point. Individual and group access to approved applications and networks is allowed by BIG-IP APM using dynamic, per-session L7 (HTTP) ACLs. The VPE in BIG-IP APM can be used to quickly and easily create, modify, and manage ACLs.

BIG-IP APM also dynamically enforces step-up authentication to additional single- or multi-factor authentication methods. Step-up policies may be based on applications, secure portions of applications, sensitive web URIs, extending sessions, or any session variable.

Granular access policies

BIG-IP APM lets you design access policies for authentication and authorization, and, as an option, endpoint security checks, enforcing user compliance with corporate policies and industry regulations. You can define one access profile for all connections coming from any device, or you can create multiple access profiles for different access methods from various devices. For example, you can create a policy for application access authentication or dynamic ACL connections. Authorized, appropriate application, network, or cloud access is based on who the user is, how and when the user is attempting access, from where the user is attempting access, what the user is attempting to access, and the network or cloud conditions at the time access is requested.

Context-based authorization

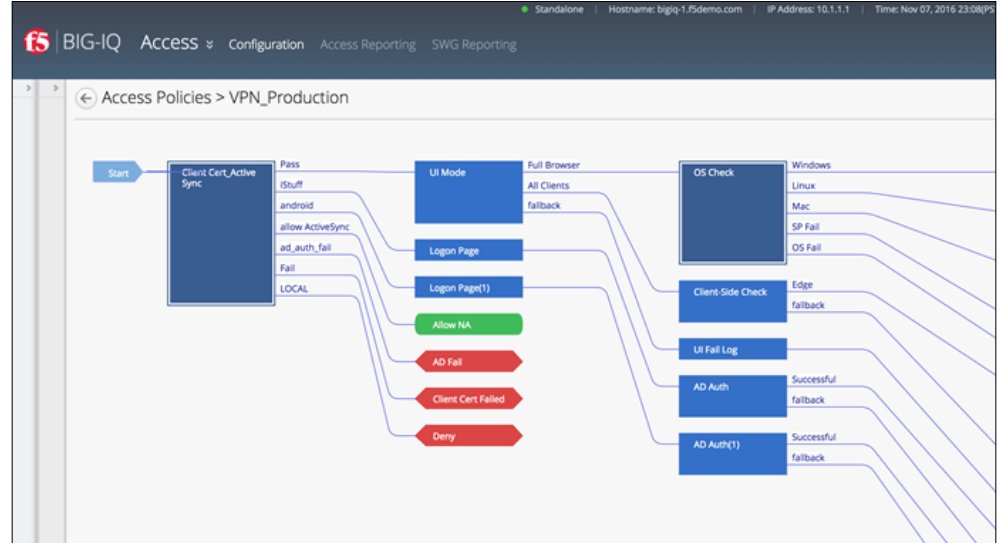
BIG-IP APM drives user identity into the network, creating a simplified, central point of control for user access. When tens of thousands of users access your applications, network, or clouds, BIG-IP APM will offload SSL encryption processing to the BIG-IP platform, provides authentication and authorization services, and optionally creates a single secure SSL connection to the application server. Authorization based on user, application, network/cloud, and threat/vulnerability context enables dynamic, secure, policy-based control over users' application, network, and cloud access.

Centralize access policy management

If you have multiple BIG-IP APM deployments, F5 BIG-IQ® Centralized Management will help you to efficiently manage them. It can manage policies for up to 100 BIG-IP APM instances, enabling you to import, compare, edit, and update granular access policies across multiple user devices.

With BIG-IQ Centralized Management and BIG-IP APM, you can import configurations from a master “source” BIG-IP APM instance, simplifying access policy distribution. You may also edit device- or location-specific objects directly on BIG-IQ Centralized Management and have them propagate throughout your BIG-IP APM deployment. You can easily view the differences between current and proposed access configurations.

Figure 3: BIG-IQ Centralized Management enables the import, comparison, editing, and updating of access policies across multiple devices from a single interface.



API AND CREDENTIAL PROTECTION

APIs and user credentials are two of the most exploited threat vectors. APIs are the connective tissue in modern application architectures. Attackers are leveraging APIs to launch attacks, because they are ripe for exploitation: Many organizations expose APIs to the public and their supply chain partners, or they inadvertently leave them unprotected. User credentials are like the keys to the kingdom: All an attacker has to do is steal one set of user credentials, and they enjoy unfettered access to your organization's network, clouds, and apps. BIG-IP APM delivers protection for both APIs and user credentials.

Protecting APIs

While attackers are exploiting APIs to launch myriad attacks, organizations can ensure API security via authentication, especially if it's adaptable and protected by consistent, flexible authentication and authorization policies. BIG-IP APM enables secure authentication for REST or SOAP APIs. It also ensures appropriate authorization actions are taken. BIG-IP APM integrates existing OpenAPI, or "swagger" files, saving you time, human resources, and cost when developing API protection policies, while ensuring accurate API protection policies are in place.

Protecting credentials

User credentials need to be protected at all times because, unfortunately, all it takes is for an attacker to steal your credentials once, and they can access your network, cloud, devices, and apps. BIG-IP APM's credential protection, as part of an optional license of BIG-IP DataSafe™, secures credentials from theft and reuse. It protects against Man-in-the-Browser attacks with real-time, adaptable login encryption, and obfuscates user credentials entered into its Webtop. BIG-IP APM, in conjunction with BIG-IP DataSafe, renders the credentials unreadable and unusable, even in the unlikely event an attacker successfully steals them. BIG-IP APM also ensures login security for all applications associated via federation.

ENHANCE VISIBILITY AND REPORTING

An in-depth view of logs and events provides access policy session details. With reports available through BIG-IQ Centralized Management, BIG-IP APM helps you gain greater visibility into application access and traffic trends, aggregate data for long-term forensics, accelerate incident responses, and identify issues and unanticipated problems before users can experience them.

BIG-IP APM can customize reports with granular data and statistics for intelligent reporting and analysis. Examples include detailed session reports by:

- Access failures
- Users
- Resources accessed
- Group usage
- IP geolocation

Figure 4: Custom reports provide granular data and statistics for intelligent analysis.

Design Custom Report

General | Report Constraints | Sort Fields

Report Name:
Logins by Larry between 8am and 9am

Restrict report output to most recent:
10 Minutes

Select fields to include in report

| Available Fields | | Selected Fields |
|------------------|---|-------------------------|
| Add all | | Clear Move up Move down |
| AP Result | → | UTC Time |
| Client IP | ← | Component |
| Created | | Log Message |
| Local Time | | Log Level |
| PID | | Location |

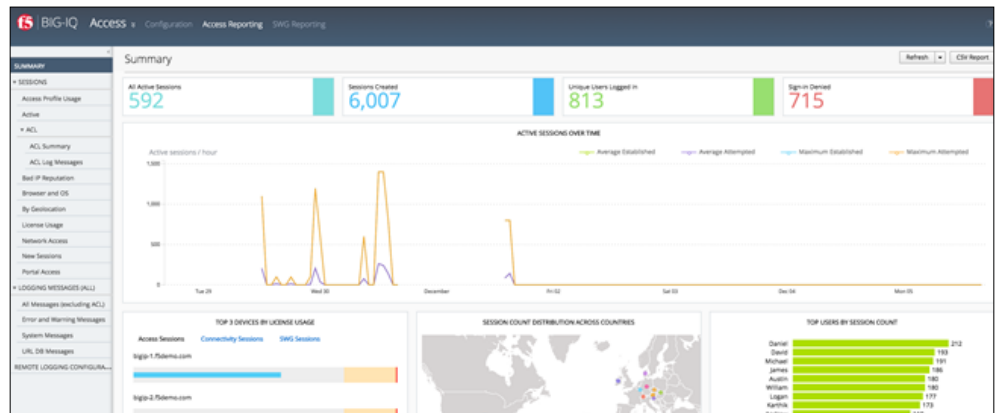
Save Cancel

Centralize reporting and logging

BIG-IP APM integrates with BIG-IQ Centralized Management to provide enhanced visibility through access reports and logs. It delivers analytical reports and logs based on devices and groups, so you can increase your insight into user access and analysis. It also helps you take quick action if required, including the termination of specific access sessions. In addition, it provides a CSV export of BIG-IP APM report data, so it's accessible for customized reports.

BIG-IQ Centralized Management's customized dashboard view can help you better envision trends and relationship contexts more easily. This improves your response time should issues arise. Through this holistic view of application and network access, you can better understand the effectiveness of the access policies you've established, locate and address weak points, and enhance your responses to issues and concerns.

Figure 5: The BIG-IQ Centralized Management comprehensive dashboard for BIG-IP APM helps you better view trends and relationship contexts.



Real-time access to health data

In addition to the access dashboard available through BIG-IQ Centralized Management for BIG-IP APM, the access policy dashboard on the BIG-IP system can provide you with a fast overview of access health. You can view the default template of active sessions, network access throughput, new sessions, and network access connections, or create customized views using the dashboard windows chooser. By dragging and dropping the desired statistics onto the window pane, you gain a real-time understanding of access health.

UNPARALLELED FLEXIBILITY, HIGH PERFORMANCE, AND SCALABILITY

BIG-IP APM delivers flexible application, network, and cloud access, keeping your users productive and enabling your organization to scale quickly and cost-effectively.

Out-of-the-box configuration wizards

BIG-IP APM helps reduce administrative costs by making it easy to quickly configure and deploy authentication and authorization services. The configuration wizard includes a set of pre-built application access and local traffic virtual device wizards. With step-by-step configuration and context-sensitive help, review, and summary, setting up authentication and authorization services on BIG-IP APM is simple and fast.

Supported platforms and licensing option

BIG-IP APM can be deployed a variety of ways to meet differing access needs. It may be:

- Deployed as an add-on module for BIG-IP LTM to protect public-facing applications
- Delivered as a standalone BIG-IP appliance or as standalone F5 VIPRION® chassis
- Included with a BIG-IP LTM Virtual Edition (VE) to deliver flexible application access in virtualized environments
- Run on High End Virtual Editions and High-Performance Virtual Editions
- Offered on a Turbo SSL platform

In addition to being licensed for these platforms, BIG-IP APM may also be licensed as the Best bundle in F5's Good-Better-Best offering, as part of F5 Enterprise Licensing Agreement (ELA) for BIG-IP VEs, and subscription licensing models.

Application firewall

With the efficient, multi-faceted BIG-IP platform, you can add application protection without sacrificing access performance. BIG-IP APM and BIG-IP Application Security Manager™ (ASM)—F5's agile, scalable web application firewall—together on a BIG-IP appliance protect applications from attack while providing flexible, layered, and granular access control. Attacks are filtered immediately to ensure application availability, security, and an optimum user experience. This integrated solution ensures compliance with local and regional regulations, including PCI DSS, so you can minimize non-compliance fine payouts and protect your organization from data loss. And, since there is no need to introduce a new appliance to the network, you save costs with an all-in-one solution.

Unprecedented performance and scale

BIG-IP APM offers SSL offload at network speeds and supports up to 3,000 logins per second. For organizations with an ever-growing base of web application users, this solution scales quickly and cost-effectively.

BIG-IP APM use is based on two types of user sessions: access sessions and concurrent connection use (CCU) sessions. Access sessions apply to authentication sessions, VDI, and similar situations. CCU is applicable for network access, such as full VPN access, application tunnels, or web access. The BIG-IP platform and the VIPRION platform—both of which support BIG-IP APM—handle exponentially more access sessions than CCU sessions in use cases such as authentication, SAML, SSO, and forward proxy. This means that if you intend to use BIG-IP APM for authentication, VDI, and the like, the number of sessions supported on VIPRION can be up to 2 million, and the BIG-IP platform can support up to one million.

F5 Virtual Clustered Multiprocessing

BIG-IP APM is available on a chassis platform and on all BIG-IP appliances. It supports the F5 Virtual Clustered Multiprocessing™ (vCMP) environment. The vCMP hypervisor provides the ability to run multiple instances of BIG-IP APM, resulting in multi-tenancy and effective separation. With vCMP, network administrators can virtualize while achieving a higher level of redundancy and control.

BIG-IP APM FEATURES

Whether running as a BIG-IP platform module or on a VIPRION chassis blade, BIG-IP APM is based on the intelligent, modular F5 TMOS® operating system. TMOS delivers insight, flexibility, and control to help you better enable application, network, and cloud access.

BIG-IP APM features include:

- Granular access policy enforcement
- Graphical Visual Policy Editor (VPE)
- IP geolocation agent (in VPE)
- AAA server authentication and high availability
- Step-up authentication, including multi-factor authentication (MFA)
- DTLS mode for delivering and securing applications
- Microsoft ActiveSync and Outlook Anywhere support with client-side NTLM
- PCoIP, Blast, and Blast Extreme proxy support for VMware Horizon, including support for Linux desktops
- SSO from smart cards for VMware Horizon deployments
- Support for VMware Horizon ONE
- Local client drive and USB redirection support for VMware Horizon
- Simplified access management for Citrix XenApp and XenDesktop, and support for Citrix StoreFront
- Native client support for Microsoft RDP client and Java RDP client
- Launch Microsoft RDP native client from Webtop
- Seamless Microsoft Exchange mailbox migration
- L7 ACL
- Protected workspace support and encryption
- Credential caching and proxy for SSO
- Java patching (rewrite) for secure access
- Flexible deployment in virtual VMware environments
- SAML 2.0 identity federation
- Support for OAuth 2.0 authorization protocol
- Integration with Oracle Access Manager (OAM)
- SSO with support for Kerberos, header-based authentication, credential caching, and SAML 2.0
- Support for SAML-based authentication using BIG-IP Edge Client and F5 Access for Android and for iOS
- SAML-artifact binding support
- SAML ECP profile support
- Simplified identity federation for applications with multi-valued attributes
- Context-based authorization with dynamic L4/L7 ACLs
- Windows machine certificate support
- Windows Credential Manager integration
- External logon page support
- Access control support to BIG-IP LTM virtual server
- Out-of-the-box configuration wizards

- Scales up to 2 million concurrent access sessions
 - Policy routing
 - Export and import of access policies via BIG-IP Centralized Management
 - Configurable timeouts
 - Health check monitor for RADIUS accounting
 - Landing URI variable support
 - DNS cache/proxy support
 - SSL VPN remote access
 - Always connected access (with BIG-IP Edge Client and F5 Access)
 - Establish an always-on VPN tunnel with Windows OS login and BIG-IP Edge Client for Windows
 - Broad client platform support: Supports several client platforms (see F5 BIG-IP APM Client Compatibility Matrices for each BIG-IP release)
 - Web browser support: Supports several web browsers (See F5 BIG-IP APM Client Compatibility Matrices for each BIG-IP release)
 - Support for endpoint security and VPN without web browser plug-ins
 - Site-to-site IPsec encryption
 - Application tunnels
 - Dynamic Webtops based on user identity
 - Integration with leading IAM vendor products (Okta, Ping Identity, VMware)
 - Authentication methods: form, certificate, Kerberos SSO, SecurID, basic, RSA token, smart card, N-factor
 - Supports Google reCAPTCHA v2 for authentication and contextual authentication
 - Endpoint posture and security checks
 - IPv6 ready
 - Virtual keyboard support
 - Style sheets for customized logon page
 - Windows Mobile package customization
 - Centralized advanced reporting with Splunk
 - vCMP
 - User credential protection
 - API protection and authorization
- TMOS features include:**
- SSL offload
 - Caching
 - Compression
 - TCP/IP optimization
 - Advanced rate shaping and quality of service
 - F5 IPv6 Gateway™
 - IP/port filtering
 - F5 iRules® scripting language
 - VLAN support through a built-in switch
 - Resource provisioning
 - Route domains (virtualization)
 - Remote authentication
 - Report scheduling
 - Full proxy
 - Key management and failover handling
 - SSL termination and re-encryption to web servers
 - VLAN segmentation
 - Denial-of-service (DoS) protection
 - System-level security protections
 - BIG-IP APM and BIG-IP ASM layering
 - F5 Enterprise Manager™ support

F5 BIG-IP PLATFORMS

Only F5's next-generation, cloud-ready ADC platform provides DevOps-like agility with the scale, security depth, and investment protection needed for both established and emerging apps. The new BIG-IP® iSeries appliances deliver quick and easy programmability, ecosystem-friendly orchestration, and record-breaking, software-defined hardware performance. As a result, customers can accelerate private clouds and secure critical data at scale while lowering TCO and future-proofing their application infrastructures. F5 solutions can be rapidly deployed via integrations with open source configuration management tools and orchestration systems.

In addition to the iSeries, F5 offers VIPRION modular chassis and blade systems designed specifically for high performance and true on-demand linear scalability without business disruption. VIPRION systems leverage F5 ScaleN® clustering technology so you can add blades without reconfiguring or rebooting.

Virtual editions of BIG-IP software run on commodity servers and support a range of hypervisors and performance requirements. These virtual editions provide agility, mobility, and fast deployments of app services in software-defined data centers and cloud environments.

See the [BIG-IP System Hardware](#), [VIPRION](#), and [Virtual Edition](#) datasheets for more details. For information about specific module support for each platform, see the latest release notes on [AskF5](#). For the full list of supported hypervisors, refer to the [VE Supported Hypervisors Matrix](#). F5 platforms can be managed via a single pane of glass with BIG-IP Centralized Management.



BIG-IP iSeries Appliances



BIG-IP Virtual Editions



VIPRION Chassis

F5 GLOBAL SERVICES

F5 Global Services offers world-class support, training, and consulting to help you get the most from your F5 investment. Whether it's providing fast answers to questions, training internal teams, or handling entire implementations from design to deployment, F5 Global Services can help ensure your applications are always secure, fast, and reliable. For more information about F5 Global Services, contact consulting@f5.com or visit f5.com/support.

MORE INFORMATION

To learn more about BIG-IP APM, visit f5.com/apm.

