Simple, Secure, and Seamless Access to Any Application, Anywhere

Applications are gateways to your critical and sensitive data. Simple, secure access to your applications is paramount, but application access today is extremely complex. Apps can be hosted anywhere—in the public cloud, in a private cloud, on-premises, or in a data center. Ensuring users have secure, authenticated access anytime, anywhere, to only the applications they are authorized to access is now a significant challenge. There are different application access methods to deal with these complexities. There are also various sources for authorized user identity, as well as dealing with applications that require modern or more traditional authentication and authorization methods, single sign-on (SSO), federation, and more, in addition to ensuring a secure, simple user access experience to support and consider.

With digital transformation touching every part of an enterprise today, native cloud and Software as a Service (SaaS) applications are now the enterprise application standard. Many organizations, though, find they’re unable or unwilling to migrate all their applications to the cloud. There may be mission-critical classic or custom applications that cannot or should not support migration to the public cloud or be easily replaced by a SaaS solution. Applications are being hosted in a variety of locations, with differing and many times disparate authentication and authorization methods that are unable to communicate with each other or work seamlessly across existing SSO or federated identity. They may be unable to support the newest identity methods, like Identity as a Service (IDaaS), and may not be equipped to support multi-factor authentication (MFA). And this doesn’t even touch on the push toward a zero trust architecture.

F5® BIG-IP® Access Policy Manager® (APM) is a secure, flexible, high-performance access management proxy solution directing global access to your network, the cloud, applications, and application programming interfaces (APIs). Through a single management interface, BIG-IP APM consolidates remote, mobile, network, virtual, web, and API access. With BIG-IP APM, you can create, enforce, and centralize simple, dynamic, intelligent application access policies for all your apps, regardless of where or how they’re hosted.
BRIDGING SECURE ACCESS TO ALL APPLICATIONS

Modern authentication and authorization protocols—including Security Assertion Markup Language (SAML), and OAuth with OpenID Connect (OIDC)—reduce user dependency on passwords, increase security, and improve user experience and productivity. However, not all applications support modern authentication and authorization protocols. Many applications, such as classic applications or custom-built applications, support classic authentication and authorization methods, such as Kerberos, header-based, and more. This further complicates application access and security. The need to support different, disparate protocols unable to share user authentication and authorization information inhibits the use of SSO and MFA, which negatively affects user experience and application security. It also makes it difficult to adapt modern corporate password management and hygiene policies, and increases organizational costs as it becomes necessary to require and manage multiple access methods.

BIG-IP APM serves as a bridge between modern and classic authentication and authorization protocols and methods. For applications unable to support modern authentication and authorization protocols, like SAML and OAuth with OIDC, but which do support classic authentication methods, like Kerberos and header-based authentication, BIG-IP APM converts users’ credentials to the appropriate authentication standard the application supports. BIG-IP APM ensures that users’ organizations can use SSO to access any application anywhere—regardless of its location (on-premises, in a data center, in a private cloud, or in the public cloud as a native cloud or SaaS application), or whether or not it supports modern or classic authentication and authorization. This decreases the number of passwords users have to create, remember, and use, which helps stem the tide of credential-based attacks. BIG-IP APM enables compliance with modern corporate policies, like periodic password changes, that help combat stolen credentials. It also decreases the cost of having to purchase and maintain separate access solutions for applications that do not or cannot support modern authentication methods.
BIG-IP APM supports identity federation and SSO options by supporting connections initiated by both SAML identity providers (IdP) and service providers (SP) leveraging SAML 2.0. It empowers administrators to centrally enable and disable user authorized access to any identity-enabled applications, regardless of where they’re hosted, saving time, and boosting administrative productivity.

Supporting the OAuth 2.0 open-standard for authorization enables BIG-IP APM to serve as a client, as an authorization delegate for SaaS applications, and to enhance the protection and authorization of APIs for web services.

INTELLIGENT INTEGRATION WITH IAM AND IDAAS

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 (CAC) and IDaaS—such as Microsoft Azure Active Directory, Okta, and others—to access all applications regardless of location or support for modern authentication and authorization. For instance, users can be 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.

F5 partners with leading on-premises and cloud-based identity and access management (IAM) vendors, such as Microsoft, Okta, and Ping Identity. This integration enables local and remote user SSO via SAML, OAuth, or FIDO2 (U2F) 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, working with its partners, F5 and BIG-IP APM work to help these organizations maintain control of on-premises user credentials. This is accomplished by creating a bridge between the IAM or IDaaS vendor’s offering and the local authentication services. This bridge, or identity provider chain, leverages SAML to federate user identity.
**SIMPLIFYING SECURE AUTHENTICATION**

Through F5’s extensive partner ecosystem, BIG-IP APM also integrates with most leading MFA solutions, including those from Duo (Cisco), Okta, Microsoft Azure Active Directory, 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. If needed, BIG-IP APM can also provide one-time password (OTP) authentication via email or SMS.

After the user has logged into an application, an additional means of authentication may be required to ensure secure access to mission-critical or particularly sensitive applications and files. This is commonly referred to as step-up authentication. 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 use additional authentication capabilities or select from our partner offerings. In addition, any session variable may be part of access policy branching (such as URL branching) per request policy. Step-up authentication policies may be based on applications, secure portions of applications, sensitive web URIs, extending sessions, or any session variable.

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.

As organizations focus on reducing user friction and increasing agility, their need to provide seamless access to all applications becomes a priority. BIG-IP APM enables organizations to reduce friction for users to remote access (SSL VPN). It also reduces friction for web applications. BIG-IP APM supports SSO across both remote access and web applications with a single login for either Apple Macs or Microsoft Windows devices (via Windows Hello for Business). Organizations can support the user login via U2F tokens (such as Yubico keys) or password-less FIDO2 via the F5 Edge Client to reduce user friction and increase application access security.
ZERO TRUST APPLICATION ACCESS

Many organizations—and maybe yours—are rapidly moving toward a zero trust security architecture. The pillars of a zero trust architecture are identity and context.

A zero trust approach to security means adopting a mindset that attackers have already infiltrated your network and are lurking, waiting for an opportunity or trigger to launch their attack. It eliminates the idea of a trusted insider within a defined network perimeter, assuming, at best, a limited secure network perimeter. It means never trusting users, even if they’ve already been authenticated, authorized, and granted access to applications and resources. A zero trust approach applies least privilege rights to user access, allowing users access rights only to the applications and resources they need to complete their tasks, and no more.

Identity and context awareness are also what define Identity Aware Proxy (IAP). IAP enables secure access to specific applications by leveraging a fine-grained approach to user authentication and authorization. IAP enables only per-request application access, which is very different than the broad network access approach of VPNs that apply session-based access, which is not a zero trust approach. With this approach, a VPN becomes optional to access applications. IAP enables organizations to create and enforce granular application access policies based on contextual attributes, for example, user identity, device integrity, and user location. IAP relies on application-level access controls, not network-layer rules. Configured policies reflect user and application intent and context. IAP requires a strong root of trusted identity to verify users and to stringently enforce what they’re authorized to access.

Identity Aware Proxy is foundational to both a zero trust architecture and to F5 BIG-IP APM. BIG-IP APM and F5 Access Guard, a browser extension that coordinates with BIG-IP APM, deliver Identity Aware Proxy using a zero trust validation model on every application access request. Providing authenticated and authorized users secure access to specific applications, it leverages F5’s best-in-class access proxy. BIG-IP APM centralizes user identity and authorization. Access is based on the principles of least privilege.

Through IAP, BIG-IP APM examines, terminates, or authorizes application access requests. Policies within BIG-IP APM can be created to:

- Verify user identity
- Check device type and posture
- Validate user authorization
- Confirm application integrity and sensitivity
- Confirm time and date accessibility
• Limit or halt access if the user’s location or device posture is deemed incorrect, inappropriate, or insecure

• Request additional forms of authentication—including multi-factor authentication (MFA)—if the user’s location or the sensitive nature of the applications or its data warrant it

• And more

Data from user and entity behavior analytics (UEBA) and other API-driven risk engines can be integrated seamlessly via BIG-IP APM’s HTTP Connector, adding another level of security and application access control.

BIG-IP APM checks user device security posture via F5 Access Guard. However, BIG-IP APM and F5 Access Guard go beyond simply checking device integrity at authentication, delivering continuous, ongoing device posture checks to ensure user devices not only meet but adhere to endpoint security policies throughout the application access session. If BIG-IP APM detects any change in device integrity, it can either limit or stop application access, halting potential attacks before they can even be launched.

BIG-IP APM enforces access authentication using access control lists (ACLs) and authorizes users with dynamically applied layer 4 and layer 7 ACLs per session. Both L4 and L7 ACLs are supported based on the posture of users’ devices as a policy enforcement point (PEP). Individual and group access to approved applications and networks is allowed by BIG-IP APM using dynamic, per-session L7 (HTTP) ACLs.

A guided configuration workflow allows organizations to host web applications protected by Identity Aware Proxy on a webtop, giving users a single catalog of all applications to which they’re authorized. It offers a seamless user experience, as users can access all their applications from a single user interface, regardless of where the application is hosted. It also simplifies an administrator’s workflow, enabling them to easily pick, choose, and modify the applications made accessible to specific user groups.

BIG-IP APM, through IAP, also simplifies application access for remote or home-based workers, better enables and secures application accessibility, and optionally eliminates the need for VPNs.

**ROBUST ENDPOINT SECURITY**

BIG-IP APM inspects and assesses users’ endpoint devices before authentication and throughout a user’s application access session with F5 Access Guard. A browser extension that provides device integrity data to BIG-IP APM, F5 Access Guard examines device security posture and determines if the device is part of the corporate domain. Based on the results, BIG-IP APM will apply dynamic ACLs to deploy context-based security. BIG-IP APM and F5...
Access Guard include 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.

**RISK-BASED ACCESS USING THIRD-PARTY RISK ENGINES (HTTP CONNECTOR)**

Many organizations have deployed third-party user and entity behavior analytics (UEBA) or risk engines. The ability to leverage an existing UEBA or risk engine to infuse real-time analytics and risk data within access control policies can help organizations ensure that access to networks, clouds, applications, and even APIs are regulated based on a risk profile. It’s also important to address risk-based access to networks, clouds, apps, and APIs that’s triggered by a variety of relevant variables.

Through HTTP Connector, BIG-IP APM integrates seamlessly with third-party UEBA and risk engines, leveraging their risk assessment via REST APIs as part of its policy-based access controls. This enables risk-based access to networks, clouds, apps, and APIs, further enhancing BIG-IP APM’s Zero Trust IAP solution. BIG-IP APM’s HTTP Connector leverages user group, domain, and network-based triggers to increase the enforceability of risk-based access. Risk-based access enhances security, providing greater visibility and analytics to determine whether to grant or deny access to your networks, cloud, applications, and APIs.

**INTEGRATING WITH AZURE ACTIVE DIRECTORY CONDITIONAL ACCESS**

F5 BIG-IP APM and Microsoft Azure Active Directory (AD), when deployed together, enable seamless, secure access to all applications, regardless of where they’re hosted or the type of authentication—modern or traditional—they use. BIG-IP APM and Microsoft Azure Active Directory have also extended application access security by integrating Microsoft Azure AD Conditional Access and BIG-IP APM. Microsoft Azure AD Conditional Access is a tool used by Azure AD to bring signals together in order to create and make access decisions and enforce organizational policies. Policies at their simplest are “if-then” statements: If a user wants to access a resource, then they must complete an action. By leveraging Azure AD Conditional Access policies in conjunction with BIG-IP APM, organizations can apply the right access controls when needed during users’ application access sessions to keep their organization...
and applications secure. Working together, Azure AD Conditional Access serves as the policy engine delivering real-time evaluation with BIG-IP APM serving as the enforcement point. BIG-IP APM and Azure AD Conditional Access unite to deliver continuous integrity and validation, and robustly enforce dynamic access control.

![Figure 1: F5 BIG-IP APM seamlessly integrates Microsoft Azure Active Directory’s Conditional Access to deliver an even more granular layer of access security to better secure zero trust environments.](image)

**PROTECTING APIS**

APIs are the connective tissue in modern application architectures. Attackers are leveraging APIs to launch attacks because they’re ripe for exploitation. Many organizations expose APIs to the public and their supply chain partners or they inadvertently leave them unprotected.

While attackers are exploiting APIs to launch attacks, organizations can ensure API security through strong 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 supports and imports OpenAPI 3.0 (Swagger) files, saving time and cost when developing API protection policies, while ensuring accurate API protection policies are in place. Quotas, allow-lists, and deny-lists can be configured for rate limiting API requests.
SECURING CREDENTIALS

User credentials are like the keys to the kingdom: All an attacker needs to do is steal one set of user credentials and they can enjoy unfettered access to your organization’s network, clouds, 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 (MitB) attacks with real-time, adaptable login encryption, and encrypts user credentials entered into its webtop login. 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.

BIG-IP APM also supports server authentication via Client Certificate Constrained Delegation (C3D). By employing C3D, BIG-IP APM addresses certificate-based authentication, limiting the need for and use of credentials. With C3D, organizations can implement stronger encryption protocols and the latest key exchanges, as well as employ client certificate authentication, enable end-to-end encryption in reverse proxy environments, leverage Perfect Forward Secrecy (PFS), and validate client certificates using Online Certificate Status Protocol (OCSP).

UNIFYING ACCESS FROM ANY DEVICE

BIG-IP APM is positioned between your applications and your users, creating a strategic application access control point. APM protects your public-facing applications by providing granular policy for identity- and context-aware user access, while consolidating your access infrastructure. It secures remote and mobile access to applications, networks, and clouds via SSL VPN or zero trust application access via Identity Aware Proxy. BIG-IP APM converges and consolidates all access—network, cloud, application, and API—within a single management interface. It also enables and simplifies the creation of easy-to-manage dynamic access policies.

BIG-IP APM creates a dynamic web-based application portal or webtop. The BIG-IP APM webtop shows and enables access only to the applications authorized for and available to a user based on their identity and context—regardless of where the applications are hosted—on-premises, in a data center, in a private cloud, in a public cloud, or offered as a service. This dynamic, user-specific application portal or webtop simplifies application access and enhances the user experience.

F5 BIG-APM enables secure access to applications, networks, and clouds via the BIG-IP Edge Client and F5 Access. The BIG-IP Edge Client is available for Apple macOS, Microsoft Windows, Linux platforms, and Chromebooks. F5 Access is an optional mobile client for ensuring secure access from mobile devices supporting Apple iOS and Google Android, and is available for download from the Apple App Store or Google Play.
BIG-IP Edge Client and F5 Access integrate with leading mobile device management (MDM) and enterprise mobility management (EMM) solutions—including VMware Workspace ONE (AirWatch), Microsoft Intune, and IBM MaaS360—to perform device security and integrity checks and to deliver per-app VPN access without user intervention. Context-aware policies are assigned based on a device’s security state as determined by the MDM or EMM solution. These policies enable, modify, or disable application, network, and cloud access from the device. Hardware attributes may be mapped to a user’s role to enable additional access control decision points. A browser cache cleaner automatically removes any sensitive data at the end of a user’s session.

BIG-IP APM enables Datagram Transport Layer Security (DTLS) mode, supporting DTLS 2.0 for remote connections that secure and tunnel delay-sensitive applications. It supports IPsec encryption for traffic between branch offices or data centers. Per-app VPN via an application tunnel through BIG-IP APM enables access to a specific application without the security risk of opening a full network access tunnel.

The dynamic split tunneling capability in BIG-IP Edge Client provides a simple way for administrators to dynamically exclude Zoom, Microsoft 365, or Webex traffic in APM network access tunnels. Real-time, latency-sensitive traffic won’t be slowed down by going through a tunnel and being encrypted, which could affect user experience. This also enables administrators to easily manage which traffic they want to go through tunnels and how that traffic should be handled.

**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), allowing Microsoft RDP to be available on non-Windows platforms, including macOS, Linux, Apple iOS, and Google Android. It also enables Microsoft RDP to work with any Microsoft, Apple, or Google web browser, or RDP app installed. BIG-IP APM also supports Citrix Virtual Apps and Desktops, and Citrix StoreFront, consolidating support for Citrix desktop and application virtualization infrastructure. It also delivers security proxy access for VMware Horizon. Administrators can control 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.
**VISUAL POLICY EDITOR (VPE)**

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 dynamic access policies in just a few clicks. BIG-IP APM’s VPE can define rules per URL path. By centralizing and simplifying the management of contextual policies, you can efficiently direct 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 identity- and context-based access policies.

BIG-IP APM lets you design access policies for authentication and authorization, as well as endpoint security checks, enforcing user compliance with corporate policies and industry regulations. One access profile may be defined for all connections coming from any device, or you can create multiple access profiles for different access methods from various devices. The VPE in BIG-IP APM can be used to create, modify, and manage ACLs quickly and easily.

**ACCESS GUIDED CONFIGURATION (AGC)**

BIG-IP APM includes an Access Guided Configuration (AGC) capability that simplifies the deployment and management of application access. The AGC guides administrators through a step-by-step process of setting up and deploying BIG-IP APM, saving your organization deployment time and cost. BIG-IP APM’s AGC also empowers administrators to quickly and simply onboard and operationally manage the integration of classic mission-critical applications, such as SAP ERP, Oracle PeopleSoft, Oracle E-Business Suite (EBS), and
Oracle JD Edwards with Microsoft Azure AD. BIG-IP APM's AGC eliminates numerous steps previously required to bridge the access gap between applications that support modern authentication and apps that support classic authentication methods—greatly reducing the administrative overhead involved in modernizing those applications.

**Figure 3:** BIG-IP APM's Access Guided Configuration saves deployment time and cost.

**Figure 4:** F5 BIG-IP APM’s Access Guided Configuration enables quick, simple onboarding and management of custom applications and classic applications, such as SAP ERP, Oracle PeopleSoft, Oracle E-Business Suite (EBS), and Oracle JD Edwards with Microsoft Azure AD.
CENTRALIZE ACCESS POLICY MANAGEMENT

For organizations with multiple deployments of BIG-IP APM, F5 BIG-IQ® Centralized Management will efficiently manage them. It manages 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 propagate them throughout your BIG-IP APM deployment. You can easily view the differences between current and proposed access configurations.

Figure 5: BIG-IQ Centralized Management enables the import, comparison, editing, and updating of access policies across multiple devices from a single interface.

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 customizes 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 6: Custom reports provide granular data and statistics for intelligent analysis.

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, increasing 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 helps to better envision trends and relationship contexts. This improves response time should issues arise. This holistic view of application and network access enables a better understanding of the effectiveness of established access policies, makes it easier to locate and address weak points, and enhance responses to issues and concerns.

![Big-Iq Access Policy Manager](image)

**Figure 7:** The BIG-IQ Centralized Management comprehensive dashboard for BIG-IP APM helps you better view trends and relationship contexts.

The access policy dashboard on the BIG-IP system also provides 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 windowpane, 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.

BIG-IP APM can be deployed a variety of ways to address your specific access needs. BIG-IP APM 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 part of 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.

BIG-IP APM supports F5 Virtual Clustered Multiprocessing™ (vCMP). 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 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, IAP, 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. If you intend to use BIG-IP APM for authentication, VDI, and similar scenarios, supported sessions on VIPRION can reach 2 million, and the BIG-IP platform can support up to 1 million.
BIG-IP APM Features

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

**BIG-IP APM FEATURES INCLUDE:**

**Access Policies**
- Full proxy
- Granular access policy enforcement
- Creating and managing identity- and context-aware policies
- Policy routing
- Identity- and context-based authorization with dynamic L4/L7 ACLs
- Risk-based access leveraging third-party Ueba and risk engines (HTTP Connector)
- Configurable timeouts
- DNS cache/proxy support
- IP geolocation agent (in VPE)
- Visual Policy Editor (VPE)
- Compatible with JavaScript Parser ES 6/7

**Authentication and Authorization Support**
- Bridging modern authentication and authorization (SAML, OAuth/OIDC) and classic authentication and authorization methods
- Authentication methods: form, certificate, Kerberos SSO, SecurID, basic, RSA token, smart card, N-factor
- Support for SAML-based authentication using BIG-IP Edge Client and F5 Access for Android and iOS
- Step-up authentication support
- Support for SAML-artifact binding
- Support for SAML ECP profile support
- Support for OAuth 2.0 authorization protocol
- Multi-factor authentication (MFA) via one-time password (OTP) solution
- Supports Google reCAPTCHA v2 for authentication and contextual authentication
- AAA server authentication and high-availability
- User credential protection
- Integrates with third-party multi-factor authentication (MFA) solutions, including Duo (Cisco) and Microsoft Azure Active Directory

**Identity Aware Proxy / Zero Trust Application Access**
- Support for Identity Aware Proxy (IAP) enabling zero trust application access
- Enables per-request application access
- Continuous endpoint integrity and security checks
- Integrates with Microsoft Azure Active Directory Conditional Access

**Identity Federation and SSO**
- SAML 2.0 identity federation support
- Simplified identity federation for applications with multi-valued attributes
- Dynamic “webtops,” based on user identity
- Microsoft Identity Platform 2.0 support
- SSO support for classic authentication (Kerberos, header-based, etc.), credential caching, OAuth 2.0, SAML 2.0, and FIDO2 (U2F)
- Integrates with third-party SSO solutions
- Credential caching and proxy for SSO
- Integrates with third-party Identity-as-a-Service (IDaaS) solutions, including Microsoft Azure Active Directory and Okta
Remote Access
- Enables zero trust application access
- SSL VPN remote access
- Always connected access
- Establish an always-on VPN tunnel (with Windows OS login and BIG-IP Edge Client for Windows)
- Site-to-site IPsec encryption

API Protection
- API protection and authorization
- Supports and imports OpenAPI 3.0 (Swagger) files
- Supports configuration of quotas, allow-lists, and deny-lists for rate limiting API requests

Simplified Administrative Experience
- Access Guided Configuration (AGC)
- Simplified guided access support for classic applications, including SAP ERP, Oracle PeopleSoft, Oracle E-Business Suite (EBS), and Oracle JD Edwards
- External logon page support
- Landing URI variable support
- IPv6 ready
- Style sheets for customized logon page
- Health check monitor for RADIUS accounting
- AES128-GCM encryption

Scalability
- Scales up to 2 million concurrent access sessions

Growing Ecosystem
- Broad client platform support (see F5 BIG-IP APM Client Compatibility Matrices for each BIG-IP release)
- Robust web browser support (see F5 BIG-IP APM Client Compatibility Matrices for each release)
- Support for Identity-as-a-Service (IDaaS), including Microsoft Azure Active Directory and Okta
- BIG IP Edge Client and F5 Access integrate with VMware Workspace ONE (AirWatch), Microsoft Intune and IBM MaaS360
- Seamlessly integrates with third-party MFA, including Duo (Cisco)
- OIDC protocol support for Duo (Cisco) MFA
- Integrates with leading IAM vendor products (Microsoft, Okta, Ping Identity)
- Integrates with Microsoft Azure AD Conditional Access
- Windows machine certificate support
- Windows Credential Manager integration

Reporting and Visibility
- Export and import of access policies via BIG-IQ Centralized Management
- Centralized advanced reporting with Splunk

Virtual Appliance
- VMware Horizon View 7.13 and Horizon 8.0 support
Additional F5 Support

- vCMP
- F5 iRules® scripting language
- Access control support to BIG-IP LTM virtual server

F5 BIG-IP Platforms

Please refer to the BIG-IP System Hardware, VIPRION, and Virtual Edition data sheets 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-IQ Centralized Management.

F5 Support Services

F5 Support 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 Support Services can help ensure your applications are always secure, fast, and reliable. For more information about F5 Support Services, contact consulting@f5.com or visit f5.com/services/support.

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