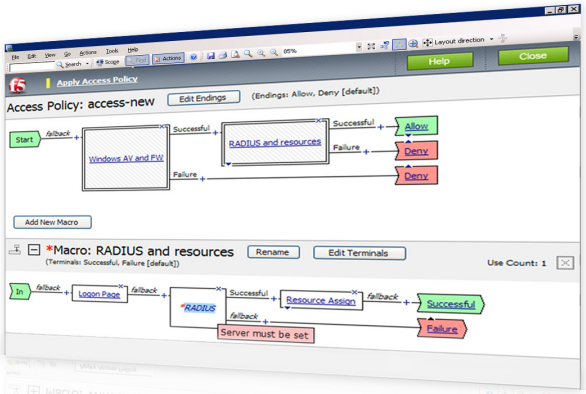
BIG-IP Access Policy Manager

DATASHEET

What's Inside



Connect to the Extended Enterprise with Confidence and Security

F5 BIG-IP® Access Policy Manager® (APM) is a secure, flexible, high-performance solution that provides unified global access to your network, cloud, and applications. With a single management interface, it converges and consolidates remote, mobile, network, virtual desktops, and web access. BIG-IP APM enables the creation and enforcement of simple, easy-to-manage, intelligent access policies.

Key benefits

Centralize identity and access control

Simplify access management with identity, context, and application-aware policies.

Unify access controls

Consolidate remote, mobile, network, virtual desktop infrastructure (VDI), and web access in one interface with adaptive identity federation, single sign-on (SSO), and multi-factor authentication (MFA).

Reduce costs

Replace proxy tiers with an integrated solution for VMware Horizon/Workspace ONE, Citrix XenApp, Microsoft Exchange, and others.

Defend the weak links

Protect against data loss, malware, and rogue device access with comprehensive endpoint posture and security checks.

Secure web access

Control access to suspicious web content and apply intelligent Forcepoint technology to defend against highly complex web threats.

Do it all at scale

No performance trade-offs for security, even in the most demanding environments.

ICSA labs CERTIFIED SSL VPN

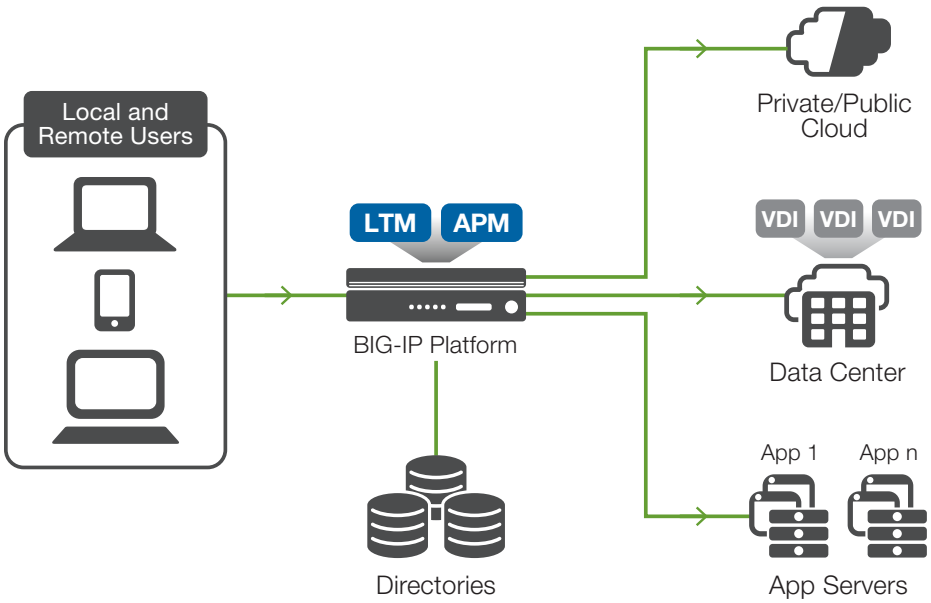
ICSA labs CERTIFIED FIREWALL - CORPORATE

Unify Global Access and Security

As your workforce grows more mobile, users need access to their applications—anywhere from any device, and often over unsecured networks. Ensuring these always-connected users have fast and secure access to applications, on-premises or in the cloud, continues to be a challenge for many organizations. By implementing policy-based access decisions, BIG-IP APM can strengthen corporate compliance with security standards, corporate controls, and industry and government regulations.

One solution for all access

BIG-IP APM is positioned between your applications and your users, delivering 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 also provides secure remote and mobile access to corporate resources from all networks and devices. BIG-IP APM converges and consolidates access within a single management interface. It also enables and simplifies the creation of policies that are easy to manage.



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

"Always connected" remote and mobile access

BIG-IP APM can be used with its optional client to enable secure remote and mobile access to applications wherever they reside, as well as networks and clouds. The integrated BIG-IP® Edge Client® provides location awareness and zone determination to deliver secure, persistent, policy-based access.

BIG-IP APM with BIG-IP Edge Client delivers secure, identity-, context-, and application-aware remote access via SSL VPN for today's remote and mobile workforce. 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. By using BIG-IP APM's VPN, your organization gains end-to-end security across your entire global infrastructure and beyond.

BIG-IP Edge Client helps ensure continued productivity whether a user is attempting to access corporate apps from home over a wireless network, giving a presentation over the corporate wireless network, in a café on guest WiFi, or docked on a LAN connection in the office. BIG-IP Edge Client automatically detects domains and reconnects even after losing a VPN connection, or it 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 Edge Client on Windows.

BIG-IP APM extends managed access for remote and mobile users to support a wide range of mobile devices. The BIG-IP® Edge Portal® application facilitates secure remote access to enterprise web applications and is available for all Apple iOS and Google Android devices. Full SSL VPN is available for Apple Mac, iPhone, and iPad devices; Microsoft Windows and Windows Phone devices; Linux platforms; and Google Android devices. The new F5 Access app is also available, empowering enterprises to deliver secure remote access via BIG-IP APM's SSL VPN capabilities for Google Chrome OS, and popular corporate devices such as Chromebooks.

When deployed with leading mobile device management (MDM) and enterprise mobility management (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 AirWatch, IBM MaaS360, and other EMM solutions—without requiring user intervention.

Eliminate browser plug-ins

Some web browsers have employed limits on the number and type of browser plug-ins that may be enabled. F5 BIG-IP APM removes the need for web browser plug-ins while still providing a friendly end user experience. This plug-in free solution can still support endpoint posture checks and network access (VPN) from web browsers.

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 can 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.

Robust endpoint security

BIG-IP APM can enable an inspection of the user's endpoint device through a web browser or through BIG-IP Edge Client to examine its security posture and determine if the device is part of the corporate domain. Based on the results, it can assign dynamic Access Control Lists (ACLs) to deploy identity-, context-, and application-aware security.

BIG-IP APM includes more than a dozen preconfigured, integrated endpoint inspection checks, including 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 Apple iOS or Google Android, BIG-IP APM's endpoint inspection checks the mobile device UDID and jailbroken or rooted status.

BIG-IP Edge Client and F5 Access integrate with leading EMM solutions—including VMware AirWatch and IBM MaaS360—to perform device security and integrity checks. Context-aware policies are then assigned based on the device's security state. These policies can

enable, modify, or disable application, network, and cloud access from a user's device. Administrators can 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.

Simplify access to authorized applications

BIG-IP APM's dynamic Webtop displays a web-based launch pad with all the applications available to a user. The content of BIG-IP APM's Webtop is dynamic, showing only those applications and resources a user is authorized to access. Webtop is customizable based on a user's identity, context, and group membership. Webtops can be set up with identity federation via Security Assertion Markup Language (SAML) and are SSO enabled, delivering a seamless user experience.

Simplify Identity Federation and Consolidate Infrastructure

BIG-IP APM simplifies and consolidates your infrastructure. The flexibility and scalability helps you to combine network access controls, identity federation, SSO, and adaptive authentication into a single application delivery solution.

Identity federation and single sign-on (SSO)

BIG-IP APM supports SSO and Kerberos ticketing across multiple domains, enabling additional types of authentication, such as U.S. Federal Government Common Access Cards (CACs) 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 after a user has been authenticated through a supported user-authentication mechanism. BIG-IP APM also delivers smart card support with credential providers, so that users can connect their devices to the network before signing in.

BIG-IP APM simplifies mobile access to protected resources by enabling remote access (VPN) authentication and authorization from Microsoft Windows, Apple Mac OS, Apple iOS, and Google Android devices—as well as devices running Chrome OS via SAML (such as Google Chromebooks). SAML-based authentication increases security, reduces user dependencies on passwords, and improves both the 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 (IdPs) and service providers. This functionality extends identity federation, as well as SSO capabilities to cloud-based applications and offers identity federation across an organization's BIG-IP products. It also empowers administrators to centrally disable user access to all identity-enabled applications, regardless of where they reside, saving time and boosting administrative productivity.

BIG-IP APM can serve as a translator, enabling SSO via SAML to applications that support SAML, as well as to those that are not SAML-enabled. For applications that do not accept SAML, BIG-IP APM can convert the authentication access to the appropriate authentication for that application. This ensures users can utilize SSO to applications—regardless of whether these apps support SAML, are on-premises, or in the cloud.

BIG-IP APM secures the transport of SAML messages by supporting SAML artifact binding, reducing the flow of SAML messages through browsers, addressing certain browser restrictions, and extending identity federation and SSO support to automatically submitted

forms that do not support JavaScript. BIG-IP APM also extends identity federation via SAML to client-based applications and other browserless 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 supports 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 application programmable interfaces (APIs) for web services.

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 their 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 EMM helps policies to be consistently applied to mobile access as well.

Automatically synchronize Exchange services

BIG-IP APM supports the synchronization of 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 (OWA), ActiveSync, and Outlook Anywhere connections, BIG-IP APM helps you consolidate infrastructure and maintain user productivity. When migrating to Exchange 2010, BIG-IP APM 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

By delivering seamless user access to web applications in a highly available and heterogeneous environment, BIG-IP APM improves business continuity and saves your organization from decreased user productivity. BIG-IP APM supports and integrates with AAA servers and user credential stores—including Active Directory, Lightweight Directory Access Protocols (LDAP), RADIUS, and Native RSA SecurID—and delivers high availability through the intelligent traffic management capabilities of BIG-IP 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 and seamlessly authenticating that user. BIG-IP APM also supports Google reCAPTCHA V2 for authentication and contextual authentication.

BIG-IP APM can help your organization deploy MFA. BIG-IP APM includes one-time password (OTP) authentication, via email or Short Messaging Service (SMS). Through F5's extensive partner ecosystem, BIG-IP APM also integrates with most leading MFA solutions, including Identity-as-a-Service (IDaaS) offerings. By integrating with your existing authentication solution, you can enjoy adaptive authentication, enabling various forms of single-factor or multi-factor authentication to be employed based on user identity, context, and the application being accessed.

BIG-IP APM enables you 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 chose from wide selection 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, which can 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 works with leading on-premises and cloud-based identity and access management (IAM) vendors, such as Ping Identity, Okta, and VMware. This integration enables on-premises and remote-user SSO—via SAML—to on-premises or data center-based applications. For organizations that do not wish to replicate their user credential store in a cloud-based application, BIG-IP APM works with IAM vendor partners to help these organizations maintain control of user credentials on-premises. 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.

With Ping Identity, BIG-IP APM can work with both PingAccess and PingFederate. This enables agent-less interaction and proxy consolidation, reduces infrastructure complexity, and delivers superior scalability while maintaining the roles and responsibilities between infrastructure security and secure IAM.

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. BIG-IP APM helps administrators gain control over the delivery and security components of enterprise virtualization solutions, enabling them to benefit from BIG-IP APM's unified access, security, and policy management. The scalable, high-performance capabilities of BIG-IP APM provide simplified access and control to users in hosted virtual desktop environments. Through these capabilities, F5 continues to deliver simple, broad virtual application and desktop support.

Simplify access to VMware virtual applications

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

Enterprises can use single sign-on (SSO) from smartcards with BIG-IP APM and VMware View Connection Server, enabling gateway consolidation 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 provides single sign-on (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 enabling BIG-IP APM to publish Citrix apps to the VMware vIDM portal. BIG-IP APM 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 integrates with the Microsoft RDP protocol, enabling Microsoft RDP access without the need to install client-side components or run Java. BIG-IP APM makes Microsoft RDP available to use on new platforms, such as Apple iOS and Google Android devices. It also enables native RDP clients on non-Windows platforms such as Apple Mac OS and Linux, where previously only a Java-based client was supported.

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

Consolidate Citrix infrastructure

BIG-IP APM supports Citrix XenApp and XenDesktop simultaneously, as well as Citrix StoreFront. This further consolidates support for the Citrix desktop and application virtualization infrastructure. For instance, in a typical Citrix XenApp or XenDesktop implementation, an administrator may 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, or 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 be updated or they risk incompatibilities. In addition, support for device or operating system-specific RDP remote access clients can be 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.

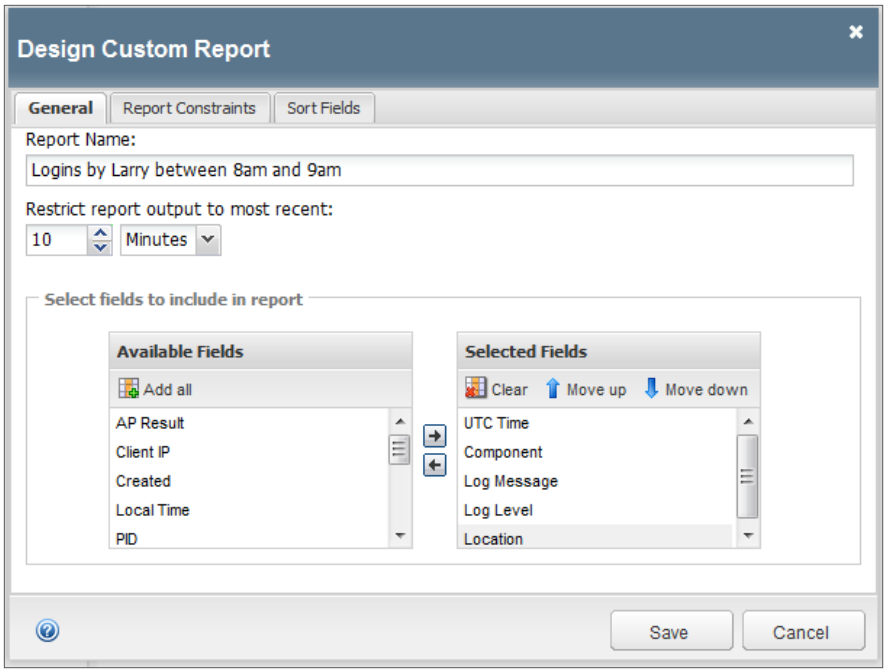
BIG-IP APM supports a Java-based, platform-independent RDP client. The client is dynamically downloadable from BIG-IP APM with support for SSO, the ability to support up to sixteen parallel monitors, and with no administration rights required on endpoint devices.

Enhance Visibility and Reporting

An in-depth view of logs and events provides access policy session details. With reports available from F5 BIG-IQ® Centralized Management, BIG-IP APM helps you gain visibility into application access and traffic trends, aggregate data for long-term forensics, accelerate incident responses, and identify unanticipated problems before users 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

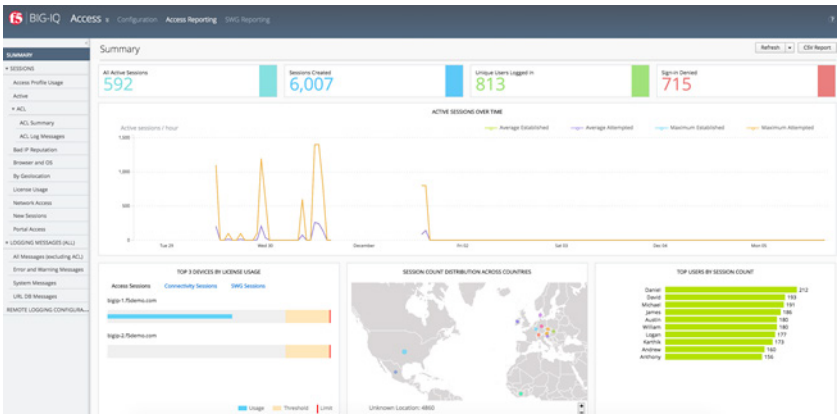


Custom reports provide granular data and statistics for intelligent analysis.

Centralize reporting and logging

BIG-IP APM integrates with BIG-IQ Centralized Management to provide visibility through access reports and logs. BIG-IQ Centralized Management 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 actions 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 provides a comprehensive dashboard for BIG-IP APM and user access. This 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 policies you've established, find and best address weak points, and enhance response to issues and concerns.



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

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.

Real-time access 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 gives you 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.

Centralize Dynamic Access Control

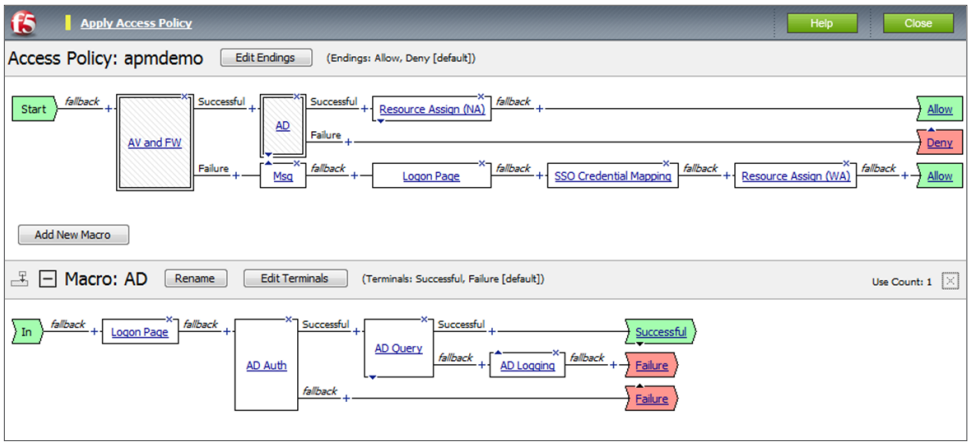
By enabling identity-, context-, and application-aware, policy-based access decisions, BIG-IP APM strengthens corporate compliance with security standards—and industry and government regulations—while ensuring users stay productive with appropriate application access.

Advanced Visual Policy Editor

The advanced, GUI-based Visual Policy Editor (VPE) in BIG-IP APM makes it fast and simple for you to design and manage granular access control policies on an individual or group basis. With the VPE, you can efficiently create or edit entire dynamic access policies with just a few clicks.

For example, you can design an authentication server policy integrated with RADIUS, 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.

The BIG-IP APM 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 a specific day, time of day, or other identity-, context-, and application-based attributes. By centralizing and simplifying the management of contextual policies, you can efficiently and cost-effectively manage access.



The BIG-IP APM advanced Visual Policy Editor makes it fast and easy to create, modify, and manage granular identity-, context-, and application-aware access policies.

Dynamic access control

BIG-IP APM provides access authentication using access control lists (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 (PEP). BIG-IP APM allows individual and group access to approved applications and networks using dynamic, per-session L7 (HTTP) ACLs. You can use the BIG-IP APM Visual Policy Editor 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 can 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, as well as optional endpoint security checking, to enforce 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 profiles for different access methods from varying devices, each with their own access policy. For example, you can create a policy for application access authentication or dynamic ACL connections. With policies in place, your network becomes identity-, context-, and application-aware: It understands who the user is, how and when the user is attempting application access, where the use is attempting to access the application from, what application the user is attempting to access, and the current network conditions at the time access is requested.

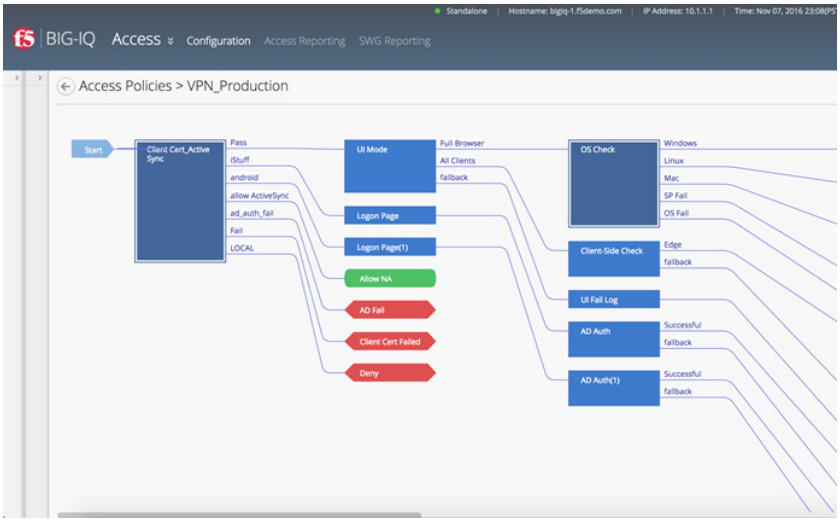
Identity-, context-, and application-based authorization

BIG-IP APM drives identity into the network, creating a simplified, central point of control over user access. When tens of thousands of users access an application, BIG-IP APM offloads SSL encryption processing, provides authentication and authorization services, and optionally creates a single secure SSL connection to the application server. Identity-, context-, and application-based authorization delivers complete, secure, policy-based control over users' application, network, and cloud navigation.

Centralize access policy management

If you have multiple BIG-IP APM deployments, BIG-IQ Centralized Management can 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. In addition, you can easily view the differences between current and proposed access configurations.



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

Secure Web Gateway Services

It's vital to ensure corporate and regulatory compliance for Internet use. F5 Secure Web Gateway Services can enforce secure web access for on-premises, remote, and mobile users. It also helps protect against web-borne malware, targeted attacks, and other insidious dangers lurking on the web.

URL filtering

URL filtering helps to ensure appropriate usage policies. Using the extensive Forcepoint database, URL filtering in Secure Web Gateway Services controls access to websites, web-based applications, protocols, and videos. Secure Web Gateway Services also filters search results based on your policy, preventing the display of offensive search results or images. URL filtering is customizable, and it helps reduce and mitigate corporate exposure to web-based threats and data leakage. BIG-IP APM provides flexibility for enterprises to allow, block, or "confirm and continue" access for certain users to the Internet, specific websites, and web applications.

URL categorization database

Secure Web Gateway Services leverages the powerful Forcepoint URL categorization engine and database that is constantly classifying tens of millions of URLs across the Internet. URL categorization is contextually-aware and applies real-time classification information against known web pages—assessing new web pages and URLs using advanced machine learning. This minimizes false positives and improves URL classification.

Web security

Secure Web Gateway Services also detects and blocks malware or malicious scripts within web pages by scanning return HTTP/HTTPS traffic. The malware engine contains web malware analytics, signatures, and heuristic detection engines that identify and eradicate general and specialized threats.

When a remote user accesses the web through a per-app VPN tunnel in BIG-IP APM, Secure Web Gateway Services protects the session as though the user was on the corporate network. Authentication, URL filtering, and malware scanning polices are applied.

Secure Web Gateway Services can also bypass or block SSL websites (based on inspection) for privacy and compliance purposes—enabling flexible control for access to SSL-encrypted websites.

Real-time threat intelligence

Leveraging the Forcepoint cloud-based threat intelligence infrastructure to deliver constant, up-to-date security information, Secure Web Gateway Services detects threats within web and social networking content. It synchronizes with Forcepoint cloud-based threat intelligence on a user-configurable schedule.

User identification

Secure Web Gateway Services keeps track of the mapping between user identity and network addresses while enabling transparent, user-based security policies through the F5 User Identity Agent. The User Identity Agent runs on a Windows-based server and pulls information from Active Directory domain controllers, enabling Secure Web Gateway Services to fully track a user's web activity by user identity or group membership.

Graphical security reporting and comprehensive logging

The graphical user interface within Secure Web Gateway Services lets system administrators view and export various security analytics reports. These reports empower administrators with total visibility of outbound and inbound web traffic, Internet use, and policy enforcement. Logs may be published through the F5 log publisher to well-known security information and event management (SIEM) solutions, including ArcSight and Splunk for longer-term storage and analytics.

Managing up to 100 Secure Web Gateway Services appliances (running with BIG-IP APM), BIG-IQ Centralized Management enables you to centrally view and manage the devices and their policies. BIG-IQ generates reports for Secure Web Gateway Services, including reports on the top blocked users, websites, categories, host names, client IPs, applications, and application families. It also enables you to track your Secure Web Gateway Services subscriptions. Data can be exported in .csv files so you may build your own reports and correlate data in other tools.

Flexible licensing and deployment options

Secure Web Gateway Services has two licensing options available. One subscription is for the URL filtering service that controls access to websites or web applications based on the categories and risks associated with the intended URLs. The second subscription includes in-line scanning of web content to detect and block threats and malware. Each is available as a one-year or three-year subscription.

Creating custom URL categories to enforce outbound web traffic access control does not require either a URL filtering or Secure Web Gateway services subscription. For malware scanning and full-scale URL filtering, however, a full Secure Web Gateway Services license, along with BIG-IP APM, is necessary. Secure Web Gateway Services can be flexibly deployed through explicit proxy and transparent proxy modes.

Unparalleled Flexibility, High Performance, and Scalability

BIG-IP APM delivers flexible application, cloud, and network access and performance. It keeps your users productive and enables your organization to scale quickly and cost-effectively.

Deployment options

BIG-IP APM can be deployed three different ways to meet a variety of access needs. It may be deployed as an add-on module for BIG-IP LTM to protect public-facing applications; it can be delivered as a standalone appliance; and it can run on a BIG-IP LTM Virtual Edition (VE) to deliver flexible application access in virtualized environments.

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 (WAF)—run together on a BIG-IP appliance to 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 helps ensure 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, BIG-IP APM 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 F5 VIPRION® platform, which support BIG IP APM, handles exponentially more access sessions than CCU

sessions in use cases such as authentication, SAML, SSO, Secure Web Gateway Services, 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 a VIPRION platform can be up to two million, and a 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, and 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:

- Portal access, app tunnel, and network access
- Granular access policy enforcement
- Advanced Visual Policy Editor (VPE)
- IP geolocation agent (in Visual Policy Editor)
- 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
- Simplified access management for Citrix XenApp and XenDesktop, and support for Citrix StoreFront
- Native client support for Microsoft RDP client and Java RDP client
- PCoIP, Blast, and Blast Extreme proxy support for VMware Horizon, including support for Linux desktops
- SSO from smart cards for VMware Horizon deployments
- Local client drive and USB redirection support for VMware Horizon
- Launch Microsoft RDP native client from Webtop
- Seamless Microsoft Exchange mailbox migration
- L7 access control list (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 for Android and BIG-IP Edge Client 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-IQ 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)
- Browser support: Supports several 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 (Ping Identity, Okta, VMware)
- Web filtering, URL categorization, real-time web malware detection and protection, and cloud-based detection of new and emerging advanced threats with F5 Secure Web Gateway Services
- Authentication methods: form, certificate, Kerberos SSO, SecurID, basic, RSA token, smart card, N-factor
- Supports Google reCAPTCHA v2 for authentication and contextual authentication
- Endpoint inspection: More than a dozen 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
- Virtual Clustered Multiprocessing (vCMP)

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 performance and for true on-demand linear scalability without business disruption. VIPRION systems leverage F5's ScaleN clustering technology so you can add blades without reconfiguring or rebooting.

Virtual editions of BIG-IP software run on commodity servers and support the range of hypervisors and performance requirements. These virtual editions provide agility, mobility, and fast deployment 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-IQ Centralized Management.

BIG-IP iSeries Appliance

VIPRION Chassis

BIG-IP Virtual Editions

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.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com

Solutions for
an application world.