Achieve Unified Access Control and Scale Cost-Effectively

Today, business resources, such as applications and data, are accessed inside and outside the traditional business perimeter. Local and remote employees, partners, and customers often access applications without context or security. A central policy control point delivers access based on context and is critical to managing a scalable, secure, and dynamic environment.

F5 BIG-IP® Access Policy Manager® (APM) is a flexible, high-performance access and security solution that provides unified global access to your applications and network. By converging and consolidating remote access, LAN access, web access, and wireless connections within a single management interface and providing simple, easy-to-manage access policies, BIG-IP APM helps you free up valuable IT resources while you cost-effectively secure and scale access.

Key benefits

**Provide unified global access**
Consolidate remote, LAN, and web access and wireless connections in one interface.

**Consolidate and simplify**
Replace web access proxy tiers and integrate with OAM, XenApp, and Exchange to reduce infrastructure and management costs.

**Centralize access control**
Use a simplified, central point of control to manage access to applications and websites through the creation and enforcement of context-aware policies.

**Ensure superior access and security**
Protect against data loss, virus infection, malware attack, and rogue device access with comprehensive endpoint posture and security checks.

**Secure web access**
Control user access to potentially dangerous websites and web applications, and secure against complex web threats using market-leading Websense technology.

**Enjoy flexibility and scalability**
Support users easily, quickly, and cost-effectively.
Unified Global Access

As the mobile workforce grows, users require access to corporate resources from an array of locations, different types of networks, and an increasing variety of devices. Ensuring secure and fast network, cloud, and application access and performance for remote users is a key challenge.

One solution for all access

BIG-IP APM is positioned between the applications and the users, creating a strategic control point in the network. BIG-IP APM protects your public-facing applications by providing policy-based, context-aware access to external users while consolidating your access infrastructure. It also provides secure remote access to corporate resources from all networks and devices.

By converging and consolidating remote access, LAN access, web access, and wireless connections within a single management interface and providing access policies that are easy to create and manage, BIG-IP APM puts IT back in control of secure network, cloud, and application access.

“Always connected” remote access

BIG-IP APM works with an optional client to enable secure remote access to networks, clouds, and applications. The state-of-the-art, integrated client, BIG-IP® Edge Client,® provides location awareness and zone determination to deliver secure, persistent, policy-based access that is unparalleled. BIG-IP Edge Client helps ensure continued user productivity whether the user is at home on a wireless network, using an air card in transit, giving a presentation over corporate wireless, in a café on guest wireless, or docked on a LAN connection. BIG-IP Edge Client can automatically detect domains and reconnect even after losing a VPN connection, or it can automatically disconnect when a LAN connection is detected. BIG-IP Edge Client also recognizes when an RSA SecurID software token is installed on a user’s Windows or Mac device, prompting the user for an RSA PIN number and seamlessly authenticating them.
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 through BIG-IP Edge Client for Apple Mac, iPhone, and iPad devices; Microsoft Windows devices; Linux platforms; and Android devices.

**Enhanced connectivity to IPv6 networks**

As the Internet continues its evolution from IPv4 to IPv6, to ensure business continuity and future growth, organizations must expand their networking capabilities to support the coexistence of IPv4 and IPv6. BIG-IP APM fully supports IPv6, delivering a true global access experience.

**Consolidated Infrastructure and Simplified Management**

By integrating enterprise-wide and cost-effective application access management with centralized application delivery directly on the BIG-IP® Local Traffic Manager™ (LTM) system, BIG-IP APM greatly simplifies the implementation of identity and access management (IAM), and authentication, authorization, and accounting (AAA) services.

**Single sign-on**

BIG-IP APM supports single sign-on (SSO) across multiple domains and Kerberos ticketing, enabling additional types of authentication, such as Federal 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 after a user has been authenticated through a supported user authentication scheme. BIG-IP APM also delivers smart card support with credential providers, supporting SSO for users with devices running Windows 7 and above, enabling them to connect their devices to the network before signing into their desktops.

Security Assertion Markup Language (SAML) 2.0 further extends BIG-IP APM SSO options by supporting connections initiated by both identity providers (IdPs) and service providers (SPs). This functionality extends SSO capabilities to cloud-based applications outside the corporate data center and also allows for identity federation across an organization’s BIG-IP platforms. BIG-IP APM thus minimizes time spent logging into multiple applications with SSO and enables a unified user portal for cloud, web, virtual desktop infrastructure (VDI), and client/server applications.

**Automatically synchronized 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, such as the Apple iPhone. 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.
Consolidated AAA infrastructure

Other authentication solutions use application coding, separate web server agents, or specialized proxies, which can present significant management, cost, and scalability issues. With AAA control directly on the BIG-IP system, 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.

Consolidated access for Oracle

BIG-IP APM integrates with Oracle Access Manager (OAM), so you can design access policies and manage policy-based access services for Oracle applications from one location. By consolidating plug-ins and web authentication proxies, this integration can help you reduce CapEx and OpEx.

Simplified access for virtual application environments

Using BIG-IP APM, administrators gain dynamic control over the delivery and security components of enterprise virtualization solutions and benefit from unified access, security, and policy management. For instance, in a typical Citrix XenApp/XenDesktop implementation, an administrator can replace Citrix authentication management, Secure Ticket Authority (STA), NetScaler, and XenApp Services sites (required for Citrix sourced enterprise deployment) with BIG-IP APM.

BIG-IP APM supports VMware Horizon View and Citrix XenApp/XenDesktop simultaneously, as well as other technologies in the mix. In addition, BIG-IP APM provides a single, scalable access control solution that includes both remote and LAN access policy and control with no configuration changes required to back-end servers. The solution can also be extended to other applications to achieve a simplified, lower-cost, highly scalable enterprise infrastructure.

Advanced reporting

An in-depth view of logs and events provides access policy session details. With reports from technology alliance partner Splunk—a large-scale, high-speed indexing and search solution—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 is capable of providing customized 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.

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. It creates a base set of objects as well as an access policy for common deployments, and it automatically creates branches in the configuration to support necessary configuration objects. With step-by-step configuration, 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

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.

Dynamic and Centralized Access Control

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

The advanced, GUI-based Visual Policy Editor (VPE) makes it fast and simple to design and manage granular access control policies on an individual or group basis. With the VPE, you can quickly and efficiently create or edit entire dynamic access policies with a few simple 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 enables you to customize user access rules according to your organization’s geolocation policy. The VPE also can define additional rules per URL path to, for example, enable a policy to restrict application, network, and cloud access based on IP address or on specific day, time of day, or identity-based attributes. By centralizing granular, contextual policy control, the VPE helps you manage and control access more cost-effectively.

![Visual Policy Editor](image)

The advanced Visual Policy Editor makes it easy to create 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. BIG-IP APM allows individual and group access to approved applications and networks using dynamic, per-session L7 (HTTP) ACLs. You can use the Visual Policy Editor to quickly and easily create ACLs.

Access policies

With BIG-IP APM, you can design access policies for authentication and authorization, as well as optional endpoint security checking, to enforce user compliance with corporate policies. You can define one access profile for all connections coming from any device, or you can create multiple profiles for different access methods, 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 context-aware: It understands who the user is, how and when the user is attempting application access, where the user is attempting to access the application from, and what the current network conditions are at the time of access.
Context-based authorization

By driving identity into the network, BIG-IP APM provides 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. Context-based authorization delivers complete, secure, and policy-based control over users’ navigation.

Superior Security

By making context-aware, policy-based access decisions, BIG-IP APM strengthens corporate compliance with security standards, corporate controls, and industry and government regulations, ensuring that users can stay productive with appropriate web access.

VPN technologies

BIG-IP APM works with the optional BIG-IP Edge Client to provide SSL VPN remote access for mobile and remote workers. For remote connections, it offers a Datagram Transport Layer Security (DTLS) mode, which is well suited for securing and tunneling applications that are delay sensitive. For traffic between branch offices or data centers, IPsec encryption is enabled. By using VPN technologies in the BIG-IP APM unified access solution, organizations gain end-to-end security across their entire global infrastructures.

Strong endpoint security

BIG-IP APM can deliver an inspection engine through the browser or through the optional BIG-IP Edge Client to examine the security posture of an endpoint device and determine whether the device is part of the corporate domain. Then, based on the results, it can assign dynamic access control lists to deliver context-aware security. The solution includes more than a dozen preconfigured, integrated endpoint inspection checks, including OS type, antivirus software, firewall, file, process, and registry, as well as device MAC address, CPU ID, and HDD ID. For mobile devices running Apple iOS or Google Android, the endpoint inspection engine checks the mobile device UDID and if the mobile device has been jailbroken or rooted. Administrators can map hardware attributes to a user’s role to allow additional decision points for access control. A browser cache cleaner will automatically remove any sensitive data at the end of a user’s session.

Dynamic webtops

The dynamic webtop displays a list of web-based applications available to a user after authentication. The content of the webtop is dynamic in the sense that only resources for which the user is authorized are displayed to the user. The webtop is customizable based on a user’s identity, context, and group membership. Webtops can be set up with SAML-enabled SSO to deliver a seamless user experience.

Application tunnels

If an endpoint doesn’t comply with your defined security posture policy, an application tunnel can provide access to a particular application without the security risk of opening a full network access tunnel. For example, mobile users can simply click their Microsoft Outlook clients to get secure access to their email, no matter where they are in the world. Application tunnels are also WAN optimized to efficiently deliver content to users.
Secure access with Java patching

Typically, a user opens a Java applet such as IBM terminal emulator, and it will open up network connections on arbitrary ports, which may be blocked by firewalls and might use SSL to secure the traffic. This makes the applet unusable by remote employees. With Java rewrite, BIG-IP APM transforms or “patches” server Java applets in real time so that clients that execute the applets will connect back through BIG-IP APM using SSL over an authenticated BIG-IP APM session. With BIG-IP APM, rewrite once and store patched Java in RAM cache, so there is no need to rewrite every time.

Comprehensive application access and security

With the efficient, multi-solution BIG-IP platform, you can add application security without sacrificing access performance. BIG-IP APM and BIG-IP® Application Security Manager™ (ASM) run together on the BIG-IP LTM appliance to protect applications from attack while providing flexible, layered, and granular access control. Attacks are filtered immediately to ensure application availability and security and an optimum user experience. This integrated solution helps you ensure compliance with local and regional regulations, including PCI DSS, so you can minimize 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.

Secure Web Gateway Services

It’s important to ensure corporate compliance policies for Internet use and appropriate, secure web access by authorized users, whether they are onsite or remote and whether they are conducting company business using corporate-issued or personal computing and mobile devices. F5 Secure Web Gateway Services accomplishes this.

There are two options for F5 Secure Web Gateway Services: a URL filtering service and a secure web gateway service. Each is available as a one-year or three-year subscription. The URL filtering service from F5 controls access to websites or web applications based on the categories and risks associated with the intended URLs. The secure web gateway service includes the URL filtering capability, but it also detects and blocks malware or malicious scripts hosted inside public web pages by scanning return HTTP/HTTPS traffic.

URL filtering

URL filtering helps to ensure compliance with industry and government regulations, as well as with corporate-acceptable Internet use policies. Using the extensive Websense database, URL filtering in F5 Secure Web Gateway Services controls access to websites and hundreds of web-based applications, protocols, and videos. Secure Web Gateway Services also blocks search results based on your applicable security 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.

URL categorization database

F5 Secure Web Gateway Services leverages the powerful Websense URL categorization engine and database that is constantly classifying tens of millions of URLs across the Internet and the web. URL categorization applies real-time classification information against known web pages, as well as assessing new web pages and URLs. It uses advanced machine learning, quickly assessing web pages based on content; this minimizes false positives.
and improves URL classification. URL categorization is contextually aware, using multiple characteristics to assess and determine web page and URL reputation.

### Web security

Secure Web Gateway Services also detects and blocks malware or malicious scripts within web pages by scanning return HTTP/HTTPS traffic. This is accomplished via the robust malware engine from Websense, which contains over 10,000 web malware analytics, and a collection of sophisticated signature and heuristic detection engines that identify and eradicate general and specialized threats. Secure Web Gateway Services incorporates powerful analytics that, when combined, conduct content-based and contextual evaluations for more effective detection of advanced persistent threats (APTs). It uses the content-based and contextual data gathered from web pages, combined with information from its web malware analytics, to make informed decisions and detect patterns that indicate the presence of APTs and other complex attacks that may evade other, standalone analytics. Additionally, when a remote user accesses the web through a per-app VPN tunnel in BIG-IP APM, the user’s web access also should be regulated, with enforced authentication, URL filtering, and malware scanning based on the same applied security policy as if the user had attempted any other web access. F5 Secure Web Gateway Services accomplishes this, ensuring comprehensive, coordinated web security, regardless of user access.

### Real-time threat intelligence

Leveraging Websense’s cloud-based threat intelligence infrastructure to deliver constant, up-to-date security information, Secure Web Gateway Services enables the detection of threats within web and social networking content. It sorts through all manner of web and social media content—including web pages, documents, executable files, mobile apps, and more—analyzing and processing billions of content requests daily.

Using the information culled from this data, the solution identifies and locates complex online threat trends. Secure Web Gateway Services can assess whether or not a popular website has been hijacked; monitor viral sites and content; and use news and social media topics to uncover more popular websites, viral sites, and content to assess. It takes advantage of Big Data analysis, mobile app permissions and profiles, and cloud sandbox data to predict and identify new, fast-emerging online threats. Secure Web Gateway Services synchronizes with Websense’s cloud-based threat intelligence on a user-configurable schedule.

### User identification

F5 Secure Web Gateway Services can map and track user identity to network addresses while enabling transparent user-based security policies through the F5 User Identity Agent. The F5 User Identity Agent runs on a Windows-based server, and it pulls information from Active Directory domain controllers. The F5 User Identity Agent enables Secure Web Gateway Services to fully track a user’s web activity by user identity. Secure Web Gateway Services also allows the user’s identity or group to determine whether SSL websites are bypassed or not allowed, enabling more granular control for access to SSL encrypted websites.

### Graphical security reporting and comprehensive logging

The graphical user interface within Secure Web Gateway Services allows system administrators to 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. Secure Web Gateway Services logs users’ Internet activities in forensic detail, including timestamps, source/destination IP address, user name, URLs, blocking status, and more. Logs may be published through the F5 log publisher to well-known security information and event management (SIEM) solutions, including solutions from ArcSight and Splunk. Logs from Secure Web Gateway Services also may be automatically uploaded to a Splunk cloud-based logging service and processed with a specially designed and implemented Splunk application, enabling the generation of analytic reports.

**Flexible deployment options**

F5 Secure Web Gateway Services may be flexibly deployed through explicit proxy, with the BIG-IP APM device running Secure Web Gateway Services installed anywhere in a network using a single switch port connection, requiring no disruption or network wiring changes. Secure Web Gateway Services also may be deployed through inline transparent proxy, with the forward proxy configured to intercept all HTTP and HTTPS traffic transparently, reducing the need for network configuration changes.

**Flexibility, High Performance, and Scalability**

BIG-IP APM delivers dependable, flexible application, cloud, and network access and performance to keep your users productive and enable your organization to scale quickly and cost-effectively.

**Flexible deployment**

BIG-IP APM can be deployed in 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 to deliver flexible application access in virtualized environments.

**Hosted virtual desktop**

Virtual desktop deployments have to scale to meet the needs of thousands of users and hundreds of connections per second. BIG-IP APM includes native support for Microsoft Remote Desktop Protocol (RDP), native secure web proxy support for Citrix XenApp and XenDesktop, and PCoIP for VMware Horizon View. In addition, BIG-IP APM can pass down a Java-based applet that acts as a Java RDP client and executes in the client’s browser. The Java RDP client is a quick virtual desktop infrastructure (VDI) option as requirements dictate and is a secure remote access solution for Mac and Linux users. The highly scalable, high performance application delivery capabilities of BIG-IP APM provide simplified access and control to users in hosted virtual desktop environments.

In addition, BIG-IP APM integrates the Microsoft RDP protocol, enabling Microsoft RDP access without the need to install client-side components or run Java. BIG-IP APM enables the availability and use of Microsoft RDP on new platforms, such as Apple iOS and Google Android devices, and 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. With this capability, F5 continues to deliver simplified, broad VDI support.
High availability for AAA servers

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 revenue loss that can result from decreased user productivity. BIG-IP APM integrates with AAA servers—including Active Directory, LDAP, RADIUS, and Native RSA SecurID—and delivers high availability through the intelligent traffic management capabilities of BIG-IP LTM.

Credential caching

BIG-IP APM provides credential caching and proxy services for single sign-on, so users only need to sign on once to access approved sites and applications. As users navigate, sign-on credentials are delivered to web applications, saving time and increasing productivity.

Unprecedented performance and scale

BIG-IP APM access 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 user sessions, with two types of sessions: access sessions and concurrent connection use (CCU) sessions. The access session type applies to authentication sessions, VDI, and similar situations. CCU is applicable for network access, such as full VPN access, application tunnels, or web access, for example. The F5 platforms supporting BIG-IP APM (the BIG-IP platforms and VIPRION chassis) are able to support exponentially more access sessions than CCU sessions in use cases such as authentication, SAML, SSO, Secure Web Gateway Services, forward proxy, and more. 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 2 million sessions, and a BIG-IP platform can support up to 500,000 sessions.

Virtual Clustered Multiprocessing

BIG-IP APM is available on a chassis platform and on the BIG-IP 5200v, 7200v, and 10200v appliances, and it supports a Virtual Clustered Multiprocessing (vCMP®) environment. The vCMP hypervisor provides the ability to run multiple instances of BIG-IP APM. This allows for multi-tenancy and effective separation. With vCMP, network administrators can virtualize while achieving a higher level of redundancy and control.
Big-IP APM Architecture

Running as a module on the BIG-IP platform, BIG-IP APM uses F5’s unique, purpose-built TMOS® operating system. TMOS is an intelligent, modular, and high-performing operating system that delivers insight, flexibility, and control to help you deliver and protect your web applications.

TMOS delivers:
- SSL offload
- Caching
- TCP/IP optimization
- Advanced rate shaping and quality of service
- IPv6 Gateway™
- IP/port filtering
- 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
- DoS protection
- System-level security protections
- BIG-IP APM and BIG-IP Application Security Manager (ASM) layering
- F5 Enterprise Manager support

BIG-IP APM features include:
- Portal access, app tunnel, and network access
- IP/v6 ready
- Granular access policy enforcement
- Advanced Visual Policy Editor (VPE), including geolocation agent
- AAA server authentication and high availability
- 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
- Native client support for Microsoft RDP client and Java RDP client
- Full proxy support for the VMware Horizon View PCoIP protocol
- Seamless Microsoft Exchange mailbox migration
- L7 access control list (ACL)
- Protected workspace support and encryption
- IP geolocation agent (in Visual Policy Editor)
- Credential caching and proxy for SSO
- Java patching (rewrite) for secure access
- Flexible deployment in virtual VMware environments
- Integration with Oracle Access Manager (OAM)
- SSO with support for Kerberos, credential caching, and SAML 2.0
- 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 Local Traffic Manager (LTM) virtual server
- Out-of-the-box configuration wizards
- Scale up to 2 million concurrent access sessions
- Policy routing
- Export and import of access policies
- Configurable timeouts
- Health check monitor for RADIUS accounting
- Clustered multiprocesing
- Landing URI variable support
- DNS cache/proxy support
- SSL VPN remote access (with optional BIG-IP Edge Client)
- Always connected access with BIG-IP Edge Client
- Easy application access with BIG-IP Edge Portal
- Broad client platform support (iPad, iPhone, Mac, Windows, Linux, Android)
- Browser support: IE, Firefox, Chrome
- Site-to-site IPsec encryption
- Application tunnels
- Dynamic webtops based on user identity
- Protected workspace
- Web filtering, URL categorization, real-time web malware detection and protection, and cloud-based detection of new and emerging APTs through F5 Secure Web Gateway Services
- Authentication methods: form, certificate, Kerberos SSO, SecurID, RSA token, smart card, N-factor
- Endpoint inspection: Windows, Mac, Linux, antivirus, and firewall checks; checks if Apple iOS- and Google Android-enabled devices are jailbroken or rooted
- More than a dozen endpoint posture and security checks
- Virtual keyboard support
- Style sheets for customized logon page
- Windows Mobile package customization
- Centralized advanced reporting with Splunk
- Virtual Clustered Multiprocessing (vCMP)
BIG-IP APM Platforms

BIG-IP APM is available as a standalone appliance or as a software add-on module to existing BIG-IP deployments. BIG-IP APM offers a range of models to suit a variety of performance demands. See the [BIG-IP Platform Datasheet](#) for details.

VPRION Platforms

BIG-IP Local Traffic Manager and Access Policy Manager are also available on the modular VPRION system. This chassis and blade architecture enables simple scalability as your Application Delivery Network grows. See the [VPRION Datasheet](#) for details.

<table>
<thead>
<tr>
<th>BIG-IP APM Standalone</th>
<th>Base Concurrent Users</th>
<th>Maximum Concurrent Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIG-IP APM VE Standalone Lab (10 Mbps)</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>BIG-IP APM VE Standalone (200 Mbps)</td>
<td>100</td>
<td>2,500</td>
</tr>
<tr>
<td>BIG-IP APM VE Standalone (1 Gbps)</td>
<td>250</td>
<td>2,500</td>
</tr>
<tr>
<td>2000s</td>
<td>100</td>
<td>500</td>
</tr>
<tr>
<td>2200s</td>
<td>100</td>
<td>2,500</td>
</tr>
<tr>
<td>4000s</td>
<td>500</td>
<td>5,000</td>
</tr>
<tr>
<td>4200v</td>
<td>1,000</td>
<td>10,000</td>
</tr>
<tr>
<td>5200v</td>
<td>2,000</td>
<td>20,000</td>
</tr>
<tr>
<td>7200v</td>
<td>4,000</td>
<td>40,000</td>
</tr>
<tr>
<td>10200v</td>
<td>8,000</td>
<td>60,000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BIG-IP APM Add-Ons</th>
<th>Base Concurrent Users</th>
<th>Maximum Concurrent Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIG-IP APM Module for BIG-IP VE</td>
<td>250</td>
<td>2,500</td>
</tr>
<tr>
<td>1600</td>
<td>500</td>
<td>1,000</td>
</tr>
<tr>
<td>2000s</td>
<td>100</td>
<td>500</td>
</tr>
<tr>
<td>2200s</td>
<td>100</td>
<td>2,500</td>
</tr>
<tr>
<td>3600, 4000s</td>
<td>500</td>
<td>5,000</td>
</tr>
<tr>
<td>3900</td>
<td>500</td>
<td>10,000</td>
</tr>
<tr>
<td>4200v</td>
<td>500</td>
<td>10,000</td>
</tr>
<tr>
<td>5000s, 5200v</td>
<td>500</td>
<td>20,000</td>
</tr>
<tr>
<td>6900</td>
<td>500</td>
<td>25,000</td>
</tr>
<tr>
<td>7000s, 7200v, 8900</td>
<td>500</td>
<td>40,000</td>
</tr>
<tr>
<td>10200v, 11000, VPRION 2400</td>
<td>500</td>
<td>60,000</td>
</tr>
<tr>
<td>VPRION 4480</td>
<td>500</td>
<td>100,000</td>
</tr>
<tr>
<td>VPRION 4800</td>
<td>500</td>
<td>200,000</td>
</tr>
</tbody>
</table>
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/services.

Simplified Licensing

Meeting your applications’ needs in a dynamic environment has never been easier. F5’s Good, Better, Best provides you with the flexibility to provision advanced modules on-demand, at the best value.

- Decide what solutions are right for your application’s environment with F5’s reference architectures.
- Provision the modules needed to run your applications with F5’s Good, Better, Best offerings.
- Implement complete application flexibility with the ability to deploy your modules on a virtual or physical platform.

(Note: F5 Good, Better, Best does not include F5 Secure Web Gateway Services.)

More Information

To learn more about BIG-IP APM, visit f5.com to find these and other resources.

Product overviews

BIG-IP Access Policy Manager

White paper

Secure Mobile Access to Corporate Applications

Technical brief

Secure iPhone Access to Corporate Web Applications

Case study

Security Company Keeps Systems Protected and Apps Accessible

Video

Web Application Access Management for BIG-IP LTM