BIG-IP Access Policy Manager

WHAT'S INSIDE

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 various sources for authorized user identity, as well as dealing with applications that require modern or traditional authentication and authorization methods, single sign-on (SSO), federation, and more, in addition to the 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 that they are unable or unwilling to migrate all of their applications to the cloud. There may be mission-critical classic or custom applications that should not or cannot support being migrated to the public cloud or be easily replaced by a SaaS application. 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 and can't work seamlessly across existing SSO or federated identity, that are unable to support the newest identity means like Identity as a Service (IDaaS), and are not equipped to support multi-factor authentication (MFA).

F5® BIG-IP® Access Policy Manager® (APM) is a secure, flexible, high-performance access management proxy solution managing 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, and web access. With BIG-IP APM, you can create, enforce, and centralize simple, dynamic, intelligent application access policies for all of your apps, regardless of where or how they are hosted.

ICSA labs CERTIFIED SSL VPN FIREWALL – CORPORATE

KEY BENEFITS

Simplify access to all apps
Bridge secure access to on-premises and cloud apps with a single login via SSO. It even works for applications unable to support modern authentication such as Security Assertion Markup Language (SAML), or OAuth and OpenID Connect (OIDC).

Zero Trust application access
Identity Aware Proxy (IAP) delivers a Zero Trust model validation for application access based on identity-awareness and granular context, securing every app access request without the need of a VPN.

Secure web access
Control access to web-based applications and web content centralizing authentication, authorization, and endpoint inspection via web app proxy.

Centralize and manage access control
Consolidate management of remote, mobile, network, virtual, and web access in a single control interface with adaptive identity federation, SSO, and MFA via dynamically enforced, context-based and identity-aware policies.

Streamlined authentication and authorization
Adaptive identity federation, SSO, and MFA employing SAML, OAuth, and OIDC for a seamless and secure user experience across all apps.

BRIDGING SECURE APPLICATION ACCESS

Modern authentication and authorization protocols—including Secure 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, NT LAN Manager (NTLM), RADIUS, 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. That in turn negatively impacts user experience and application security. It also makes it difficult to adapt modern corporate password policy of periodic password changes, and increases organizational costs as multiple access methods become necessary.

BIG-IP APM serves as a bridge between modern and classic authentication and authorization protocols and methods. For applications which are unable to support modern authentication and authorization protocols, like SAML and OAuth with OIDC, but which do support classic authentication methods, BIG-IP APM converts user credentials to the appropriate authentication standard supported by the application. BIG-IP APM ensures that users or 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 helps decrease the number of passwords users have to create, remember, and use, helping to stem the tide of credential-based attacks. It enables compliance with modern corporate policies of periodic password changes to combat stolen credentials. It also decreases the cost to organizations of having to purchase and maintain separate access solutions for applications hosted on-premises, in a data center, and in a private cloud, versus native cloud and SaaS apps.

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 are hosted, saving time and boosting administrative productivity.

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

KEY BENEFITS (CONT.)

Defend your weakest links
Protect against data loss, malware, and rogue device access with comprehensive, continuous endpoint integrity and security checks.

Protect APIs
Enable secure authentication for REST and SOAP APIs and integrate OpenAPI or "swagger" files to ensure appropriate authentication actions while saving time and cost.

Do it all at scale
Support all users easily, quickly, and cost-effectively with no performance trade-offs for security, even in the most demanding environments.

SUPPORT FOR 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 the use of IDaaS—such as Microsoft Azure Active Directory, Okta, and others—to access all applications regardless of location or modern authentication and authorization support. 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.

SUPPORT FOR MFA

Through F5's extensive partner ecosystem, BIG-IP APM also integrates with most leading MFA solutions, including those from Cisco Duo, 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. In addition, to help you deploy MFA, BIG-IP APM includes 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.

ZERO TRUST APPLICATION ACCESS

Many organizations—possibly including yours—are rapidly moving toward adoption of a Zero Trust security architecture. The pillars of a Zero Trust security 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 to launch an attack. It eliminates the idea of a trusted insider within a defined network perimeter, assuming, at best, a limited secure network perimeter. It encourages never trusting users, even if they've already been authenticated, authorized, and granted access to applications and resources. A Zero Trust security approach applies least privilege rights to user access, allowing users to access only those applications and resources they are authorized for, and restricting their access to a single application or resource at a time.

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, VPN becomes optional to access applications. IAP enables the creation and enforcement of granular application access policies based on contextual attributes, such as 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 are authorized to access.

Identity Aware Proxy is key to both a Zero Trust security architecture and to F5 BIG-IP APM. BIG-IP APM and F5 Access Guard 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 best-in-class access proxy. BIG-IP APM centralizes user identity and authorization. Authorization is based on the principles of least privileged access.

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 their 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 adding another level of security and application access control.

BIG-IP APM checks user device security posture via F5 Access Guard, a browser extension that coordinates with BIG-IP APM. However, BIG-IP APM and F5 Access Guard go beyond simply checking device integrity at authentication to deliver continuous, ongoing device posture checks, ensuring that user devices not only meet but adhere to endpoint security policies throughout application access. 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.

A guided configuration workflow allows organizations to host web applications protected by Identity Aware Proxy on a webtop, providing users a single catalog of their applications. It offers a seamless user experience, as users can access applications, regardless of where they are hosted. It also simplifies the administrative workflow, enabling administrators to easily pick, choose, and modify the applications accessible by a specific user group.

BIG-IP APM, through IAP, also simplifies application access for remote or home-based workers and 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 the user's application access with F5 Access Guard. 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 access control lists (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 their access control policies can help those organizations ensure that access to networks, clouds, applications, and even APIs, are regulated based on a risk profile. It is also important to address risk-based access to networks, clouds, apps, and APIs that is triggered by a variety of relevant variables.

Through its HTTP Connector, BIG-IP APM integrates 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.

INTELLIGENT INTEGRATION WITH IDENTITY AND ACCESS MANAGEMENT (IAM)

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 vendor's offering and the local authentication services. This bridge, or identity provider chain, leverages SAML to federate user identity.

UNIFYING ACCESS FROM ANY DEVICE

BIG-IP APM is positioned between your applications and your users, providing a strategic application access control point. It protects your public-facing applications by providing granular policy for identity- and context-aware 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. 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 includes a dynamic web-based application portal or webtop. The BIG-IP APM webtop shows only 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.

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.

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 Horizon 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. 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.

Biometrics, such as fingerprint access, are supported to open and access the F5 Edge Client. This simplifies access, since a user will no longer need to create, remember, and input a username/password credential to access the Edge Client. It also makes accessing the Edge Client more secure, as users reuse passwords or create simple username/password pairs, making them easier for attackers to hack.

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).

SEAMLESS ACCESS TO ALL APPLICATIONS

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, as well. 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 are able to 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.

STREAMLINE VIRTUAL APPLICATION ACCESS

Virtual desktop and application deployments must scale to meet the needs of thousands of users and hundreds of connections per second. BIG-IP APM serves as a gateway for virtual application environments. It includes native support for Microsoft Remote Desktop Protocol (RDP), native secure web proxy support for Citrix XenApp and XenDesktop, and security proxy access for VMware Horizon. Administrators 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.

BIG-IP APM supports two-factor authentication via RSA SecureID and RADIUS through the native client for VMware End User Computing (EUC) deployments. BIG-IP APM supports Citrix XenApp, XenDesktop, and Citrix StoreFront, consolidating support for Citrix desktop and application virtualization infrastructure. BIG-IP APM, when integrated with the Microsoft RDP protocol, enables the remote desktop access needed to install client-side components or run Java. It allows Microsoft RDP to be available for use on new platforms, such as Apple iOS and Google Android devices. It also enables native RDP clients on non-Windows platforms such as Mac OS and Linux, where previously only a Java-based client was supported. BIG-IP APM's Microsoft RDP support works with any Microsoft, Apple, or Google web browser, or RDP app installed.

PROTECTING APIs

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

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

SECURING CREDENTIALS

User credentials are like the keys to the kingdom: All an attacker has 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. 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.

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 entire 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.

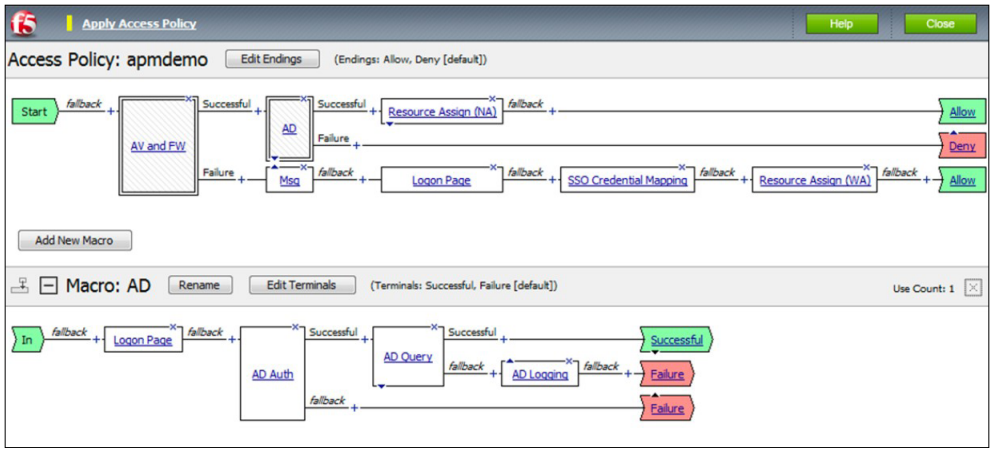

Figure 1: The BIG-IP APM advanced VPE makes it fast and easy to create, modify, and manage granular application-, user-, network/cloud-, and vulnerability context-based access policies.

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.

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

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 your administrator through a step-by-step process of setting up and deploying BIG-IP APM, saving you and your administrator deployment time and cost. BIG-IP APM's AGC also allows your administrator to quickly, simply onboard and operationally manage classic mission-critical applications, such as SAP ERP and Oracle PeopleSoft, to Microsoft Azure AD. This simplified guided access eliminates numerous steps previously required in Azure AD to bridge the access gap between applications supporting modern authentication, and apps that support classic authentication methods, greatly reducing administrative overhead involved in modernizing those applications.

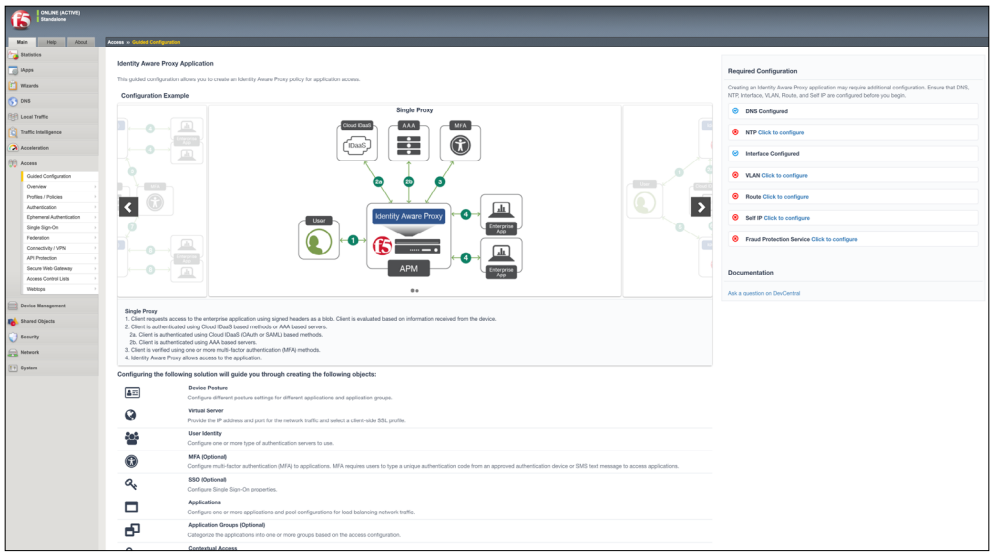

Figure 2: BIG-IP APM's Access Guided Configuration saves deployment time and cost.

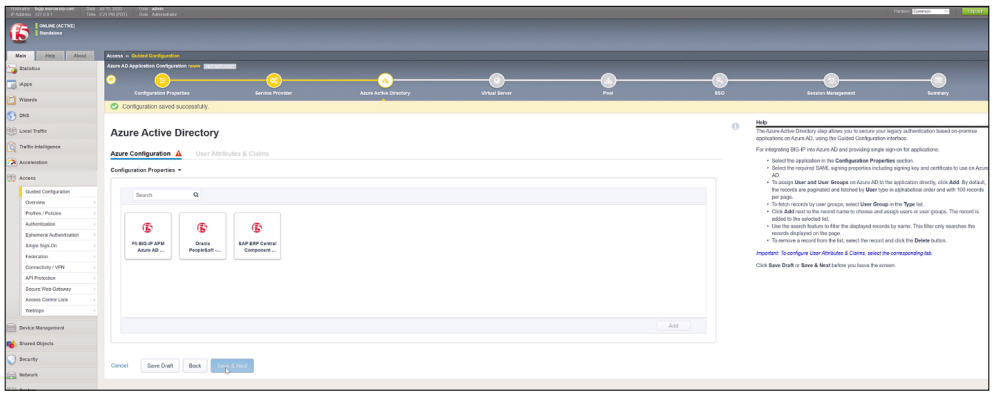

Figure 3: F5 BIG-IP APM's Access Guided Configuration enables quick, simple onboarding and management of custom applications and classic applications, such as SAP ERP and Oracle PeopleSoft, with Microsoft Azure AD.

CENTRALIZE ACCESS POLICY MANAGEMENT

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

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

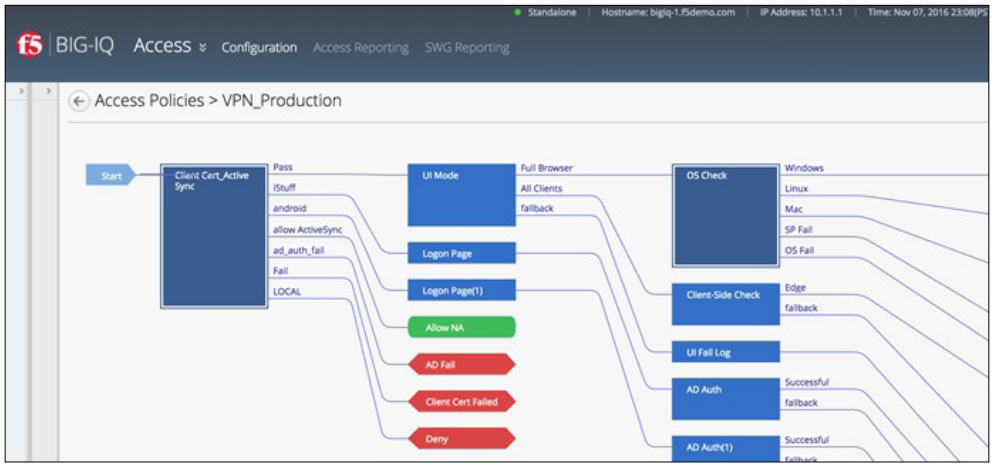

Figure 4: BIG-IQ Centralized Management enables the import, comparison, editing, and updating of access policies across multiple devices from a single interface.

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

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

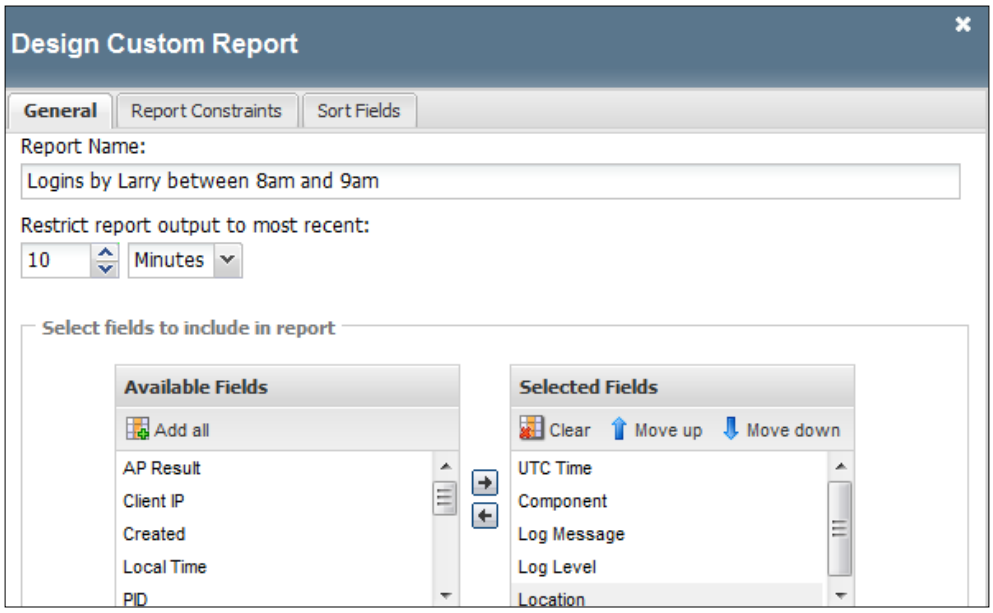

Figure 5: Custom reports provide granular data and statistics for intelligent analysis.

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, so you can increase your insight into user access and analysis. It also helps you take quick action if required, including the termination of specific access sessions. In addition, it provides a CSV export of BIG-IP APM report data, so it's accessible for customized reports.

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

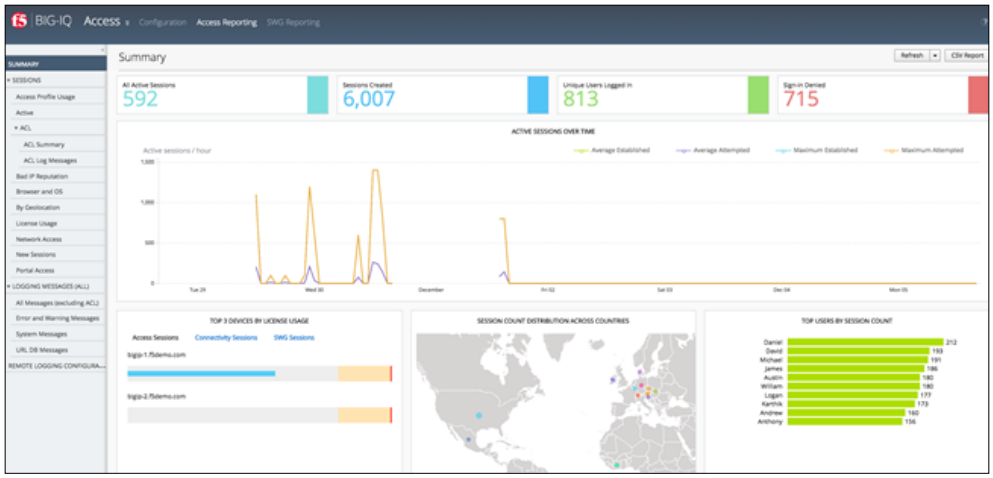

Figure 6: The BIG-IQ Centralized Management comprehensive dashboard for BIG-IP APM helps you better view trends and relationship contexts.

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

BIG-IP APM 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. This means that if you intend to use BIG-IP APM for authentication, VDI, and the like, the number of sessions supported on VIPRION can be up to 2 million, and the BIG-IP platform can support up to 1 million.

BIG-IP APM Features

Whether running as a standalone or 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:

- Granular access policy enforcement
- Creating and managing identity- and context-aware policies
- Policy routing
- Support for Identity Aware Proxy (IAP) enabling Zero Trust application access
- Context-based authorization with dynamic L4/L7 ACLs
- SAML 2.0 identity federation support
- Support for OAuth 2.0 authorization protocol
- Simplified identity federation for applications with multi-valued attributes
- 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
- Bridging modern authentication and authorization (SAML, OAuth/OIDC) and classic authentication and authorization methods
- Support for SAML-based authentication using BIG-IP Edge Client and F5 Access for Android and for iOS
- Support for SAML-artifact binding
- Support for SAML ECP profile support
- AAA server authentication and high-availability
- Step-up authentication support
- Multi- factor authentication (MFA) via one-time password (OTP)
- Seamless integration with third-party MFA solutions
- DTLS 2.0 mode for delivering and securing applications
- SSL VPN remote access
- Always connected access
- Establish an always-on VPN tunnel (with Windows OS login and BIG-IP Edge Client for Windows)
- 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)
- Continuous endpoint integrity and security checks
- Support for endpoint security and VPN without web browser plug-ins
- Site-to-site IPsec encryption
- Application tunnels
- Dynamic “webtops,” based on user identity

BIG-IP APM FEATURES INCLUDE (CONT.):

- Integration with leading IAM vendor products (Microsoft, Okta, Ping Identity)
- Authentication methods: form, certificate, Kerberos SSO, SecurID, basic, RSA token, smart card, N-factor
- User credential protection
- API protection and authorization
- Risk-based access leveraging third-party UEBA and risk engines (HTTP Connector)
- Support for Identity-as-a-Service (IDaaS), including Microsoft Azure Active Directory and Okta
- Visual Policy Editor (VPE) and Access Guided Configuration (AGC)
- IP geolocation agent (in VPE)
- Windows machine certificate support
- Windows Credential Manager integration
- External logon page support
- Access control support to BIG-IP LTM virtual server
- Scales up to 2 million concurrent access sessions
- BIG IP Edge Client and F5 Access integrate with VMware Horizon ONE (AirWatch), Microsoft Intune and IBM MaaS360
- 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
- Supports Google reCAPTCHA v2 for authentication and contextual authentication
- IPv6 ready
- Style sheets for customized logon page
- Centralized advanced reporting with Splunk
- vCMP
- F5 iRules® scripting language
- Full proxy
- BIG-IP APM and BIG-IP ASM layering

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.

BIG-IP iSeries Appliances

BIG-IP Virtual Editions

VIPRION Chassis

F5 Global Services

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

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

DC1220 | DS-SEC-598089716