IBM Tivoli Maximo Asset Management

APPLICATION READY SOLUTION GUIDE

F5 Improves the Agility, Performance, and Security of IBM Maximo Deployments

IBM® Maximo® Asset Management software unifies comprehensive asset life cycle and maintenance management on a single platform. Maximo provides insight for enterprise assets, their conditions and work processes, for better planning and control.

The F5 Application Ready Solution for Maximo, a Ready for Tivoli™ certified architecture for accelerating Maximo installations, turns your network into an agile infrastructure for application delivery. Depend on F5 to be the strategic point of control for your Maximo investment, giving you the flexibility and control to improve Maximo performance, eliminate downtime, and meet your security requirements.

F5 enables IT agility, your way.

Key benefits

Optimize Maximo performance
F5 technology can increase Maximo performance and efficiency over the WAN by more than 275%.

Enable single sign-on for Maximo
Eliminate the complexity and expense of using a separate web authorization system and streamline user experience with F5's single sign-on solution.

Gain Maximo server capacity
Extend server capacity by offloading tasks like SSL processing and compression onto F5's unified, simple to manage platform.

Deploy quickly and accurately
F5's deployment guides enable fast, accurate, and flexible deployments, allowing you to spend less time deploying Maximo and more time using it.

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

Secure your Maximo implementation
From powerful network- and protocol-level security to attack filtering, F5 protects Maximo deployments that help run your business.

Ready for
IBM. | Tivoli.
software

"IBM chose to include F5 as one of our technology partners in the ANPO offering after a rigorous product assessment. As part of an extensive vetting and technology integration process, F5 BIG-IP solutions were installed and tested in the IBM Lab in Toronto. IBM's selection of F5 illustrates the importance of Application Delivery Controller technology to ensure high quality application performance."

Cindy Klepich, Director, Network Strategy, Optimization and Integration Services in IBM's Integrated Communications Services Product Line.

Why F5?

F5 Networks is the market share leader in Application Delivery Networking, focused on ensuring the secure, reliable, and fast delivery of IBM Maximo and other applications. The following is an overview of why so many businesses rely on F5 to be the strategic point of control for their Maximo investments.

F5 has a broad and deep partnership with IBM
- Nearly all of our IBM solutions have been co-developed directly with application experts at IBM working on-site with F5 experts, or with F5 working at IBM Innovation Centers throughout the world.
- F5 has achieved the Ready for Tivoli™ certification for our Maximo solution.
- F5 is actively engaged with product groups throughout IBM's pillars of business including WebSphere, Tivoli, Lotus, Rational, Information Management Systems (Cognos and TM1), and Technology Group and Security Systems Division.
- F5 and IBM can host customers to demonstrate our solutions at IBM Innovation Centers or F5 Technology Centers throughout the world.

F5 optimizes IBM Maximo
- F5 can reduce application response times for Maximo over the WAN by more than 275% for repeat visits.
- For initial visits, F5 reduces Maximo response times by 182%.
- F5 enables organizations to overcome WAN latency and bandwidth constraints without having to deploy multiple devices or client side software.
- The F5 solution is flexible, yet powerful enough to use for Maximo as well as other IBM applications like WebSphere, Rational, Cognos and more.

F5 increases Maximo performance by offloading SSL and other services
- Use F5 for SSL processing and certificate management to significantly increase Maximo server capacity.
- Conserve Maximo resources by performing security operations on F5 for Maximo-specific protection.
- Offload compression and caching onto F5 devices to gain Maximo server capacity.
- Aggregate millions of requests into hundreds of server-side connections with F5.

F5 ensures your Maximo deployment remains secure
- Enhance Maximo security with granular application-layer protection.
- Protect Maximo with F5's ICSA Labs certified devices, certified at both the Web Application Firewall and Network Firewall levels.
- Prevent unauthorized access and enforce anti-virus levels and other policies with pre-logon checks for web clients that ensure corporate compliance.
- Set granular, easy-to-configure secure access policies that assign permission levels depending on the user's device (such as mobile device, kiosk, or company issued PC).

F5 helps keep end users and Maximo administrators productive and satisfied
- Use one F5 device to manage all access policies, regardless of the access network.
- Stay in compliance with regulations like PCI DSS, SOX, Basel II, HIPAA, while providing the Maximo performance users and administrators expect.
- Gain a comprehensive view of users, Maximo, and the network, which helps better respond to changing business needs.

**Satellite Use Case: First visit
(8 Mbps, 700 ms latency, no loss)**

120s

100s ☐ Default
      ☐ F5 Optimized

80s

60s

40s

20s

0s
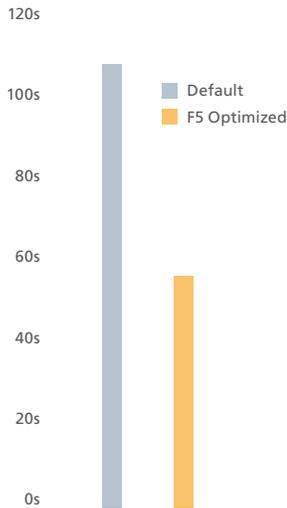
F5 improves Maximo performance over
a Satellite link by more than 180%.

**Satellite Use Case: Repeat visit
(8 Mbps, 700 ms latency, no loss)**

120s

100s ☐ Default
      ☐ F5 Optimized

80s

60s

40s

20s

0s
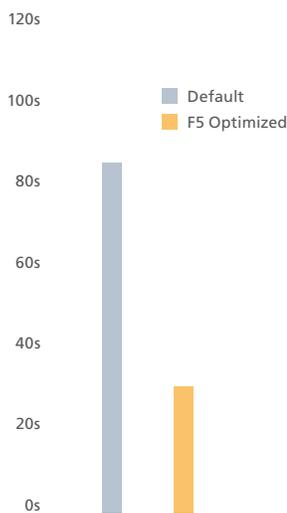
For repeat visits, the benefits of F5
are even more impressive; a 278%
improvement

Detailed Benefits and F5 Value for IBM Maximo

F5's Application Ready Solution for IBM Maximo Asset Management ensures a secure, fast and available deployment, providing the following benefits to organizations, and their end users.

F5 improves IBM Maximo end user experience and application performance

Organizations who rely on IBM Maximo count on it as a mission-critical application. Users expect Maximo to be responsive and always available, no matter where they are or what type of device they are using. This can be a daunting task for IT departments who struggle with a number of issues that have nothing to do with the application itself. Latency, bandwidth, packet loss, and other conditions across local and wide area networks are all contributing factors that lead to unresponsive applications. F5's Ready for Tivoli certified solution for IBM Maximo solves these issues by optimizing Maximo delivery over the LAN and WAN, ensuring a fast, secure, and available application experience for users no matter the location or device, enabling users to remain productive.

F5 has developed intelligent application delivery techniques that are used in tandem with WAN optimization technologies that minimize the effects of congestion, packet loss, and latency. Our devices adapt in real time to the network conditions of WAN links to fully use available bandwidth and accelerate application traffic.

Maximo users are often based around the world, connecting to a central data center. For example, users connecting from an oil platform over a satellite connection can experience slow page low times, which hinders productivity and slows down operations. By using a combination of either asymmetric web optimizations, symmetric WAN optimization, or both, F5 can vastly increase download times for a more productive user experience. As shown in the graphs on the left, our testing shows that F5 technology improves Maximo performance over Satellite links by 182% for the first visit and 278% for repeat visits. Over an OC3 link, the improvements are also impressive, with over 150% improvement for both first and repeat visits.

Improving the user experience

While Maximo uses a back-end database for session state and information retrieval, the front-end sessions through the web servers are essentially stateless. If one of the Maximo servers goes down, all user data is safe because it is stored in the database. However, the user is forced to login again because the session data is now tied to a server that is no longer available. F5 solves this issue with our integrated single sign-on solution, so users only have to sign in once, no matter which server handled the initial session. With F5, single sign-on, acceleration, security, and more are all built into a single device, which improves the experience of the administrator as well.

F5 helps reduce complexity in data centers and increase performance for end users with technology that ensures web browsers only download truly dynamic and unique content by eliminating the download of repetitive data and browser conditional requests for static data that is incorrectly considered dynamic. Additionally, adaptive compression, data deduplication, and protocol acceleration, all allow F5 to effectively maximize throughput and bandwidth.

Increasing Maximo server capacity

One of the highlights of F5's Application Ready Solution is ability to enable Maximo to achieve maximum efficiency by taking on many of the duties each server traditionally has to perform. For example, offloading SSL encryption onto F5 devices frees Maximo from the CPU-intensive task of encrypting and decrypting secure data, thus increasing server capacity.
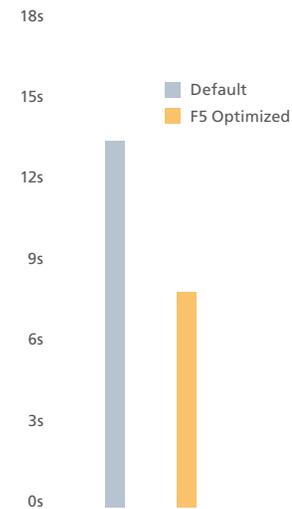
With the migration to 2048-bit keys, this becomes even more important, as these larger keys can reduce server performance 4-8 times more than 1024-bit keys. F5 SSL offload and acceleration can mitigate the impact of 2048-bit keys to help optimize the performance and capacity of your Maximo deployment.

And SSL processing is not the only task F5 can offload from the Maximo servers. F5's high-powered devices include customized hardware and software specifically designed for offloading tasks like compression and caching. By offloading these burdensome, repetitious tasks onto F5's centralized and powerful devices, Maximo has more processing power to use on asset management.

F5 technology can further increase Maximo capacity by pooling connections to the server. F5 devices can aggregate millions of requests into hundreds of server-side connections. This ensures connections can be efficiently handled by the servers and can significantly increase server capacity.

Easy implementation and management

As a part of F5's Application Ready Solution for IBM Maximo, we have carefully configured, tested, and tuned our devices with Maximo and documented the procedures in our deployment guide. This allows administrators to quickly and accurately configure F5 devices, knowing that they are using a tested and F5 approved configuration. We continually retest and tune the solution, ensuring the best possible platform for organizations with Maximo deployments.

F5 provides advanced tools that make it easy to manage our devices while maintaining flexibility and control of your infrastructure. F5 devices include a graphical reporting engine to display real-time historical statistics by the hour, day, week, or month. The dashboard reports statistics on CPU and memory usage, connections, and throughput with an easy-to-read graphical view. We make security compliance easy and save valuable IT time by enabling the exporting of policies for use by offsite auditors. Auditors working remotely can view, select, review, and test policies, without requiring critical time and support from the web application security administrator.

F5 helps simplify system management with a modular platform that consolidates security, acceleration, access, and availability on one device. This platform offers tremendous scalability and customization, allowing organizations to start with one specific function that meets the current business need and budget, and add more capacity and functionality as application and business demands change.

F5 enhances application security for IBM Maximo

Because Maximo is an asset management application, it can be a target for malicious users. Hackers and bots are using sophisticated attacks that are focused on specific applications. These attacks are perpetrated at the application layer and appear to be completely legitimate requests, easily passing through most network firewalls. F5 provides comprehensive security for your Maximo deployment, ensuring your valuable assets remain secure.

Protect Maximo from known and unknown threats

Before users even connect to Maximo, F5's comprehensive endpoint security for remote access gives the best possible protection for (and from) remote users. F5 technology prevents infected PCs, hosts, or users from connecting to your network and applications, and delivers pre-login endpoint integrity checks and endpoint trust management.

F5 security devices report previously unknown threats (such as brute force and zero-day attacks), mitigate web application threats, and remediate vulnerabilities found by 3rd party

OC3 Use Case: Repeat visit
(155 Mbps, 15 ms latency, no loss)

18s

15s

Default
F5 Optimized

12s

9s

6s

3s

0s

Over an OC3 link, F5 improves Maximo performance by over 150%

4

scanners (such as IBM Rationale AppScan), shielding the organization from data breaches. Our full inspection and event-based policies deliver a greatly enhanced ability to search for, detect, and apply numerous rules to block known L7 attacks. F5 also supports DNSSEC, which adds an additional layer of security and prevents DNS hijacking and cache poisoning.

Secure and optimize Maximo data over the WAN

F5 ensures site-to-site data security with the ability to symmetrically encrypt all data between local and remote F5 devices. This secure connection not only secures data between F5 devices, but significantly improves transfer rates, reduces bandwidth, and offloads applications for more efficient WAN communication. This technology can be used to secure and optimize user data transfer between sites and aid in data backup across the WAN.

F5 uses encrypted tunnels and deduplication to increase security and performance for remote users
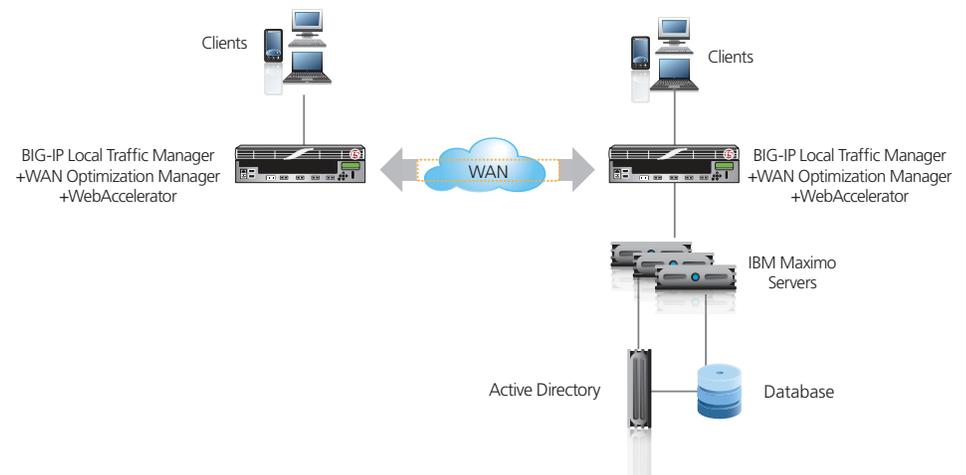
Safeguard sensitive information

F5 devices are certified by ICSA Labs at both the application firewall and network firewall levels, ensuring you are receiving the best possible protection for Maximo and your entire network. F5's intelligent security and remote auditing helps organizations comply with industry security standards, including PCI DSS, HIPAA, Basel II, and SOX, in a cost effective way—without requiring multiple appliances, application changes, or rewrites.

For example, with PCI reporting, F5 lists security measures required by PCI DSS 1.2, determines if compliance is being met, and details steps required to become compliant if not. F5 also integrates with leading security vendors for vulnerability assessment, auditing, and real-time and database reporting to provide security breach reviews, attack prevention, and compliance. For example, F5 integrates with IBM's application-security and risk management solution, Rational AppScan, to provide rapid remediation of detected vulnerabilities

Providing unified security enforcement and access control for IBM Maximo

The F5 Application Ready Solution for Maximo allows you to converge and consolidate remote access, LAN access, and wireless connections within a single management interface, and provide easy-to-manage access policies, helping you free up valuable IT resources and scale cost effectively. F5's single sign-on and endpoint inspection increase security while improving user experience.

Single sign-on for Maximo deployments

F5's integrated single sign-on provides a secure, seamless end user experience. First, F5 endpoint security technology can inspect the connecting device on a extremely granular level and grant users access to specific parts of Maximo depending on their entitlements, on the device they are using, or location from which they are attempting access. Once the endpoint

F5 devices are certified by ICSA Labs at both the application firewall and network firewall levels, ensuring you are receiving the best possible protection for Maximo and your entire network.

check passes, the user is logged on and the F5 devices securely store Maximo session credentials, passing them to Maximo when needed; all transparent to the end user. This ensures a user is required to sign in only once for any given session.

Granular control for Maximo

Another important aspect of F5's universal access approach is the ability to divide the network itself into various segments to protect and monitor access from one segment to the other. At the network level, you can use IP addresses, VLANs, MAC addresses, and packet filtering mechanisms to define practically any combination of network security policy based on any network parameter, such as originating or destination VLAN, IP address, and protocol. You can refine this security with strict access rules based on authentication results or application responses.

F5 provides organizational efficiency and an easy way to scale management by allowing our devices themselves to be partitioned into administrative domains. This enables organizations to assign varying degrees of administrative rights and views to each device. For example, the application owner for Maximo can be given permission to only view or modify objects that reside in the Maximo domain.

Enabling seamless business continuity and disaster recovery for IBM Maximo

Successful organizations expect the unexpected, and they plan for it. Network outages, hardware failures, and natural disasters can all damage an otherwise healthy business, putting critical data at risk, interrupting services, and causing significant loss of revenue. F5 solutions can help you create a strong business continuity and disaster recovery plan for Maximo and your other applications, so you can be prepared for seamless, uninterrupted operation and avoid excessive downtime and reduced productivity.

F5 enables virtualized data centers, secure remote access, optimization and traffic management in an integrated fashion. F5 provides speedy replication of data across data centers to ensure database and application integrity during failovers. We accelerate remote access for users who typically access their primary site, but due to a disaster now must remotely access the backup site. Deploying F5 solutions can help organizations achieve the best RTO (Recovery Time Objectives) and better RPO (Recovery Point Objectives).

Comprehensive and cohesive solution

F5 has the industry's most comprehensive solution for site failover and business continuity. In addition to performing comprehensive site application availability checks, you can define the conditions for dynamically and transparently shifting all traffic to a backup data center, failing over an entire site, or controlling only the affected applications. This includes geolocation (finding the best Maximo site based on user location with respect to available sites) and site resilience (real-time knowledge of the health of each Maximo site and when to failover to a backup site).

Even a minor "disaster", such as a hardware failure of a single server, can cause expensive downtime. F5 makes hardware, software, and service failures inconsequential by automatically detecting failures and transparently directing traffic away from the troubled server. Once the issue has been resolved, F5 devices automatically detect the server and resume sending traffic to it. This can also be useful for patch management or maintenance windows. Administrators can easily remove groups of devices from the F5 pool, perform patching or other maintenance while other devices remain in service. Once the maintenance is complete, those servers go back in the pool, and the remaining servers are taken down for maintenance, all completely transparent to end users, and with zero downtime.

F5's Application Ready Solution for IBM Maximo Asset Management: Explore it. Deploy it. And run your business with it.

F5 Global Configuration Diagram for IBM Maximo Asset Management

The following logical diagram shows a global configuration using the F5 suite of products to optimize, secure, and deliver IBM Maximo deployments over the WAN and LAN.
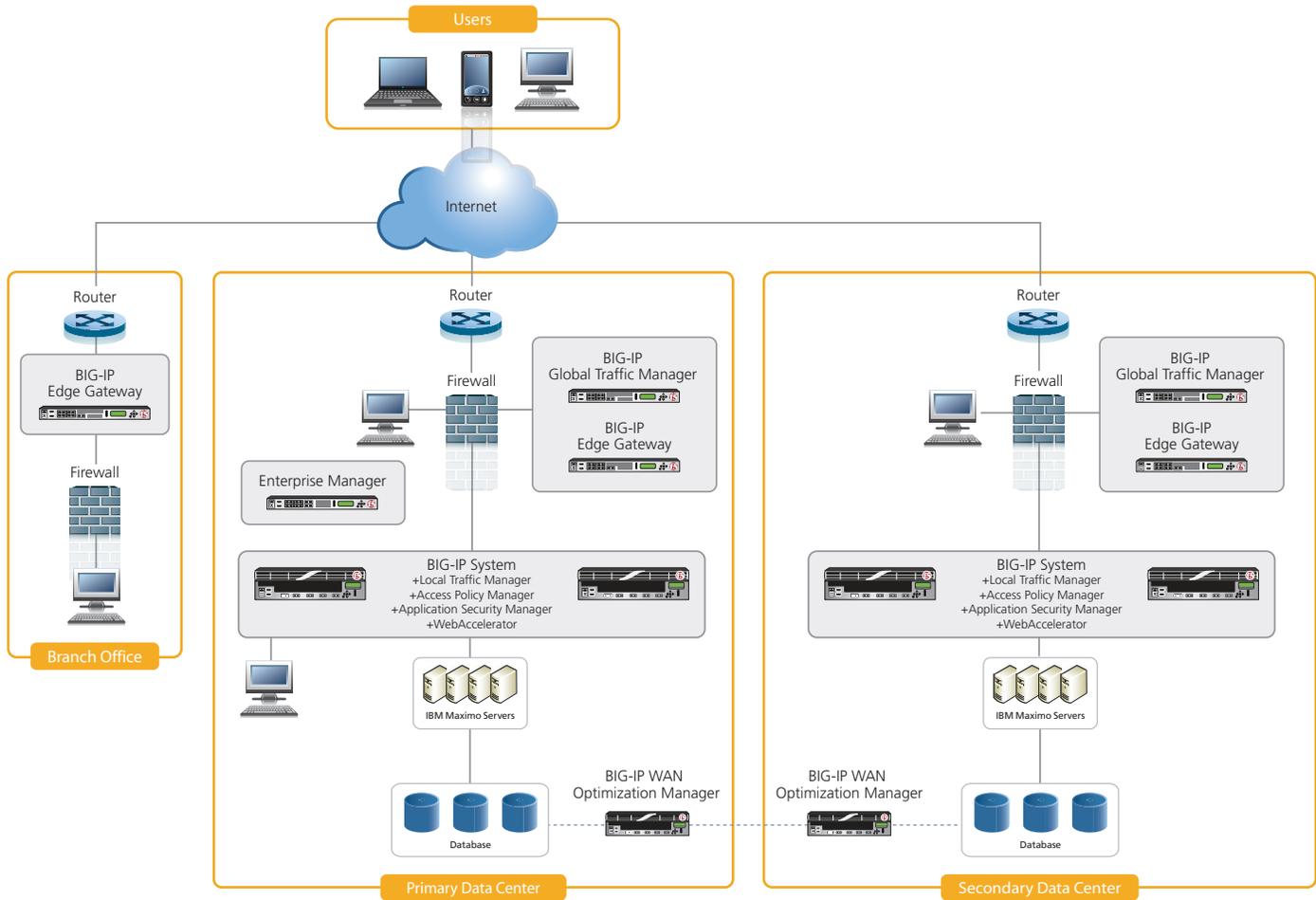
More Information

To learn more about F5's Application Ready Solution for IBM Maximo Asset Management, use the search function on F5.com to find these and other resources.

IBM Tivoli Page

IBM Tivoli

Deployment Guides

IBM Tivoli Maximo Asset Management

IBM Solutions Page on DevCentral

http://devcentral.f5.com/ibm

F5 Product Offerings

BIG-IP Product Family (Application Delivery Controller)

FirePass (SSL VPN)

Enterprise Manager (F5 Device Management)

ARX Series (File Virtualization)

Data Manager (File Virtualization)

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