



What's Inside

- 2 Boost Security for Employees and the Enterprise
- 3 Reduce IT Overhead
- 3 Encourage Employee Compliance
- 4 Improve Employee Productivity
- 4 Minimize Costs
- 5 F5 Services
- 5 More Information

Safely Extend the Enterprise to Personal Mobile Devices

With the advent of the smartphone, enterprises were pushed into the bring-your-own-device (BYOD) era. As organizations struggled to secure data and resources, IT was forced to manage employees' personally owned mobile devices and associated data—in addition to corporate data and applications. Current mobile device management (MDM) solutions focus on controlling the device and deploying agents to provide device-level VPN corporate network access. The problem: your mobile employees are subject to corporate visibility and control of their personal information, while your IT department is forced to manage and transport data and applications that aren't essential to your business operations.

F5 helps you address these challenges with F5® Mobile App Manager (MAM), a mobile application management and access solution that securely extends the enterprise to personal mobile devices. F5 MAM manages apps and secures data while satisfying the needs of both your employees who rely on their mobile devices, and your enterprise. For employees, F5 MAM safely separates personal data and usage from corporate oversight for a simpler, more flexible and productive experience. And for your IT department, F5 MAM minimizes the burden of ensuring that corporate data is secure on personal devices.

Key benefits

Boost security for the enterprise and the user

With F5 MAM, you can deliver secure access and encryption to corporate data and apps, while leaving employees' personal data and apps separate and untouched.

Reduce IT overhead

F5 MAM eliminates the need for IT to manage enterprise-issued mobile devices and the associated infrastructure.

Encourage employee compliance

Through secure, separate enterprise apps, F5 MAM lets employees make the most of the native mobile device experience while minimizing enterprise security risks.

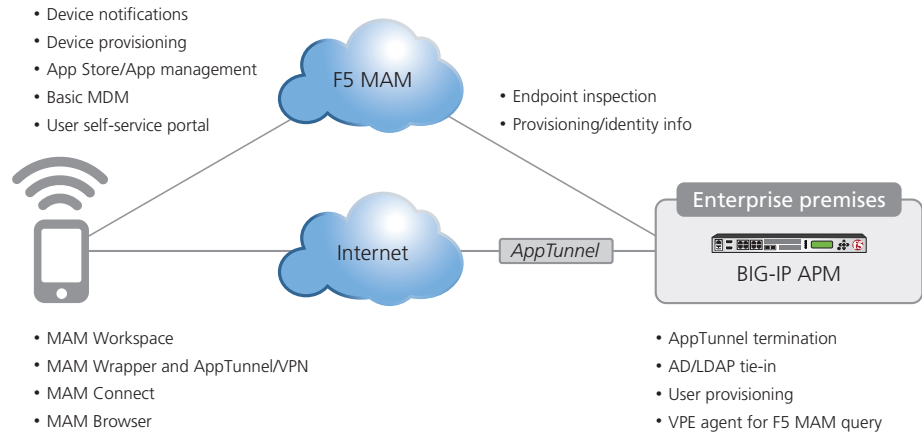
Improve employee productivity

Employees can collaborate from any location, at any time, making the most of every work day.

Lower costs

F5 MAM helps you take full advantage of BYOD benefits and associated cost savings, while reducing help desk costs.

The F5 MAM hybrid architecture combines cloud-based app management with on-premises application tunnel termination.



F5 MAM includes:

- **Mobile App Manager Wrapper and AppTunnel/VPN**—A security wrapper automatically applied to select enterprise applications, MAM Wrapper ensures separation of business and personal elements, as well as provisions AppTunnel/VPN (application-specific network access).
- **Mobile App Manager Connect**—A secure, encrypted personal information manager (PIM) that integrates with Microsoft Exchange to deliver enterprise email, calendar, contacts, and notes—separate from personal PIM apps.
- **Mobile App Manager Browser**—A secure, managed browser for enterprise use, completely separate from the user's personal browser.
- **Mobile App Manager App Store**—An easy-to-administer enterprise content and application store.
- **Mobile App Manager Workspace**—A virtual enterprise workspace available for Android devices that keeps enterprise data and apps separate. For iOS devices, F5 MAM offers equivalent security and management functionality using application wrappers.

Boost Security for Employees and the Enterprise

F5 MAM is equally compelling for employees and IT because it safely separates personal data and usage from corporate oversight. Employees retain the freedom to take full advantage of their devices, without having to disable useful features. IT manages only the enterprise subset of the data and apps on the device, and is not burdened with transporting and managing personal information.

Application Wrapping

F5 MAM's application wrapping capabilities simplify the deployment of select apps to an employee's mobile device. MAM Wrapper is applied to the target app automatically and post-compile, so there is no need to touch the application code. MAM Wrapper enables data to be shared across enterprise-secured apps. For example, when an employee attempts to open an attachment via the email component of MAM Connect, the wrapped version of the corresponding viewer application will be used to open that attachment.

MAM Wrapper includes data-at-rest encryption and restricted copy and paste functionality. MAM Wrapper also includes AppTunnel secure data transport enabled by the AppTunnels feature of F5 BIG-IP® Access Policy Manager® (APM), and more. Wrapped applications can be

made available via the MAM App Store, a customizable portal that IT can use to push select apps. Content distribution can be differentiated based on platform or user group membership.

Reduce IT Overhead

F5 MAM employs a Software-as-a-Service (SaaS)-based delivery mechanism to help streamline your deployment. With a SaaS-based solution IT doesn't need to deploy, configure, or manage additional hardware. Simply purchase the licenses you need, and application management can occur instantly. Key components and capabilities of F5 MAM including application wrapping, application tunnels, and flexible policy management provide a comprehensive app security and management environment.

Application Tunnels

F5 MAM helps organizations shift from secure device-level connectivity to secure app-level connectivity, while ensuring that the enterprise footprint on a personal mobile device is limited to the enterprise data and applications accessed through the device. You can now replace existing device-level VPNs with application-specific VPNs, by taking advantage of BIG-IP APM AppTunnels, which enable a single encrypted connection to specific services such as Microsoft Exchange. As a result, only the enterprise subset of the overall personal device data and applications are secured and transported by the corporate network, leaving the connectivity of the device itself, and the management of personal data and applications, to the device owner.

Flexible Policy Management

Administrators can manage application access globally, by groups, or by individual devices. IT can push down policy and configuration requirements to your organization's divisions quickly and easily, while enforcing compliance. This allows administrators to maintain consistent policies across all devices in the enterprise, and gives your organization a mobile IT solution that extends from data and applications on the endpoint into the cloud and the data center.

Encourage Employee Compliance

Many enterprise security policies for MDM, such as disabling the camera on a mobile device, may severely limit the employee's enjoyment of or most productive use of the device. Another concern is that most MDM products are designed to examine the entire device and all of its contents, making no distinction between business and personal. Not only is this a potential privacy issue, there is a risk to the user of losing personal data (such as photos or contacts) should the enterprise find it necessary to wipe the device clean of enterprise data. In general, the more you attempt to control employees' personal mobile device use, the less likely they are to willingly comply with your organization's security regulations. This can result in a significant barrier to adoption.

Secure Enterprise Footprint

F5 MAM removes this barrier by letting employees work with their devices as they wish. F5 MAM doesn't inspect content or disable features; instead, it creates a secure footprint on the device that is reserved for enterprise data and access. Each enterprise application is securely wrapped, which restricts incorrect or inappropriate use. Secure access is automatically provisioned by the application itself, and in the event that a device is lost or stolen, IT can wipe clean only the enterprise data from the device and leave personal data untouched.

Improve Employee Productivity

When employees are empowered to use their own devices for work, they tend to resolve business issues and make important decisions faster, in real-time. Because employees can collaborate from any location at any time, and use key productivity and communications apps on their devices, they tend to be more efficient and more productive during the work day.

Secure Access to Productivity Apps

MAM Connect provides employees with secure mobile access to corporate email, calendar functionality, and contacts through Microsoft Exchange ActiveSync. Much care has been taken to replicate, and in some cases improve upon the usability and experience of the native email clients provided with mobile devices. Time-sensitive emails can be addressed immediately, from any location, and instant access to global address lists makes it easy for users to find and contact the people they need within the organization.

Minimize Costs

With F5 MAM, organizations can eliminate the need to issue corporate mobile devices and deploy the associated infrastructure—such as the servers that enable them—thereby reducing CapEx and OpEx. When combined with the productivity gains that BYOD brings, this trend can provide your enterprise with a significant advantage. Separating or segregating enterprise from personal data and applications also results in fewer help desk calls.

F5 Services

F5 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 Services can help you achieve IT agility. For more information about F5 Services, contact consulting@f5.com or visit f5.com/services.

More Information

To learn more about F5 MAM, use the search function on f5.com to find these and other resources.

White paper

[BYOD 2.0: Moving Beyond MDM](#)

Video

[Inside Look: Mobile App Manager](#)

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

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

