IBM Security Solutions
Thought Leadership White Paper

Addressing NIST and DOD requirements for Mobile Device Management (MDM)

Essential capabilities for secure mobility

Overview

The National Institute for Standards and Technology (NIST) and the Defense Information Systems Agency (DISA) have taken leading roles in exploring requirements for Mobile Device Management (MDM) systems for government agencies.

Mobile devices, particularly smartphones, are exceptionally vulnerable to security breaches. They are easily lost, are filled with unknown applications, communicate over untrusted networks, and are often purchased by users without regard to IT standards and security features.

MDM products and platforms can help mitigate these vulnerabilities. But managing mobile devices is a complex subject with many sub-topics, including policy management, secure communications, secure storage, device authentication, remediation and auditing.

In this white paper we will look at NIST and DISA efforts to articulate requirements for Mobile Device Management.

We will:

- Review the special risks of managing mobile devices described in the NIST draft report *Guidelines for Managing and Securing Mobile Devices in the Enterprise* (NIST Special Publication 800-124 Revision 1, draft, July 2012).
- Outline high-level capabilities that should be provided by MDM systems, as listed in the same document.
- Look at a selection of the detailed MDM requirements listed in *Mobile Device Management (MDM) Server Security Requirements Guide*, draft version 1 from DISA.
- See how an MDM platform, IBM® MobileFirst® Protect Devices (formerly MaaS360®), can help organizations address those requirements.

Special risks of mobile devices

Why are mobile devices risky, and why is it so important to manage them?

An excellent overview of the risks inherent in mobile devices is provided in section 2.2 of NIST Special Publication 800-124 Revision 1 (draft), *Guidelines for Managing and Securing Mobile Devices in the Enterprise.*[1] This section, titled "High-Level Threats and Vulnerabilities," outlines the risks, and also suggests the technologies needed to mitigate them.

Table 1 is a summary of the risks and mitigation strategies. Readers can consult pages 3-6 of the NIST*Guidelines* document for the details.

Vulnerabilities	Mitigation Strategies
Lack of physical security controls	
"…The devices' mobile nature makes them much more likely to be lost or stolen than other devices…[O]rganizations should assume that mobile devices will be acquired by malicious parties who will attempt to recover sensitive data either directly from the devices themselves or indirectly by using the devices to access the organization's remote resources."	• Encryption of data stored on the device. • Authentication of users attempting to access the device or resources accessible through the device.
Use of untrusted mobile devices	
"Many mobile devices, particularly those that are personally owned (bring your own device, BYOD), are not necessarily trustworthy. Current mobile devices lack the root of trust features (e.g., TPMs)...There is also frequent jailbreaking and rooting of mobile devices,which means that the built-in restrictions on security, operating system use, etc. have been bypassed…"	• Restrict or prohibit use of BYOD devices. • Fully secure each organization-issued phone before allowing it to be used. • Employ "technical solutions for achieving degrees of trust, such as running the organization's software in a secure, isolated sandbox on the phone, or using device integrity scanning applications."
Use of untrusted networks	
"…Communications systems…such as Wi-Fi and cellular networks…are susceptible to eavesdropping, which places sensitive information transmitted at risk of compromise. Man-in-the-middle attacks may also be performed to intercept and modify communications..."	• Encrypted communications. • Mutual authentication to verify the identities of endpoints.
Use of applications created by unknown parties	
"Mobile devices are designed to make it easy to find, acquire, install, and use third-party applications…Organizations should plan their mobile device security on the assumption that unknown third-party mobile device applications downloadable by users should not be trusted."	• Prohibit all installation of third-party applications. • Implement whitelisting to prohibit installation of unapproved applications. • Implement a secure sandbox to isolate the organization's data and applications from all other data and applications on the mobile device. • Prohibit or restrict browser access, or use a separate browser within a secure sandbox.
Interaction with other systems	
"Mobile devices may interact with other systems in terms of data synchronization and storage…[such as] connecting a mobile device to a desktop or laptop…[or] automatic backups of data to a cloud-based storage solution… [T]he organization's data is at risk of being stored in an unsecured location outside the organization's control; transmission of malware from device to device is also a possibility."	• Prohibit all installation of third-party applications. • Implement whitelisting to prohibit installation of unapproved applications. • Implement a secure sandbox to isolate the organization's data and applications from all other data and applications on the mobile device. • Prohibit or restrict browser access, or use a separate browser within a secure sandbox.
Use of untrusted content	
"Mobile devices may use untrusted content that other types of devices generally do not encounter. An example is Quick Response (QR) codes… [M]alicious QR codes could direct mobile devices to malicious websites…"	• Educate users on the risks inherent in untrusted content. • Restrict peripheral use on mobile devices, such as disabling camera use in order to prevent QR codes from being processed.
Use of location services	
"…[M]obile devices with location services enabled are at increased risk of targeted attacks because it is easier for potential attackers to determine where the user and the mobile device are, and to correlate that information with other sources about who the user associates with and the kinds of activities they perform in particular locations."	• Disable location services. • Prohibit use of location services for particular applications such as social networking or photo applications.

Table 1: Vulnerabilities and mitigation strategies from NIST SP 800-124 Revision 1

Mobile Device Management capabilities – four categories

The NIST's *Guidelines for Managing and Securing Mobile Devices in the Enterprise* document also does a good job summarizing some of the capabilities that should be provided by an MDM system. Many of these are similar to the capabilities expected in laptop and other systems management products, but there are a few areas where the requirements for managing mobile devices are significantly different, notably those related to controlling the download and use of apps.

We summarize the key points here. Readers can consult pages 8-9 of the NIST *Guidelines* document for more details.

General policy

An MDM system needs to manage security policies centrally. This includes restricting the use of hardware features like cameras, GPS, Bluetooth and media interfaces; restricting the use of software features such as web browsers, email clients, and app installation services; and managing Wi-Fi and Bluetooth wireless interfaces.

Policy management also includes monitoring and reporting on policy violations.

Data communication and storage

An MDM system should enforce the strong encryption of communications between the mobile devices and the organization, as well as the strong encryption of data stored on both built-in and removable storage.

An MDM system should also be able to "wipe" stored data when a device is lost or stolen, or after a number of incorrect authentication attempts.

User and device authentication

An MDM system should be able to require passwords and other forms of authentication, to set parameters for password strength and incorrect password retries, and to allow administrators to reset access remotely.

An MDM system should be able to force devices to lock themselves after a specified idle period, and to remotely lock devices left in unsecure locations.

Applications

An MDM system should be able to control applications on devices through whitelisting and blacklisting, and by installing, updating and removing applications remotely.

An MDM system should be able to prevent devices from synchronizing with local or cloud-based systems, and to prevent access to the enterprise network if the devices have been rooted or jailbroken, or have the wrong version of the MDM client.

The MDM system should be able to distribute applications from a dedicated app store.

Detailed MDM requirements – and how an MDM platform can help

The NIST *Guidelines for Managing and Securing Mobile Devices in the Enterprise* document provides very useful high-level descriptions of capabilities that should be provided by an MDM system.

But readers who want to consider more specific requirements can find them, in abundance, in another document created by the Defense Information Systems Agency (DISA) for the US Department of Defense (DOD). That document is called: *Mobile Device Management (MDM) Server Security Requirements Guide, draft version 1*.[2]

The document contains almost 300 "rules" that potentially could be applied to MDM systems used in defense organizations.

It is important to note that this Security Requirements Guide (SRG) is still an early draft, and represents a laundry list of possible requirements submitted by agencies, vendors, contributors to standards organizations, and others. No single MDM product could possibly implement all of the features suggested in the foreseeable future. However, over time this list will be consolidated and refined, and even in its current state it provides a valuable trove of ideas for what MDM systems could provide.

Here we will look at a small selection of the “rules” included in this MDM SRG. To give some structure to these suggested requirements we have grouped them into the four categories of requirements outlined in the NIST *Guidelines* document discussed earlier. (But note that this is not the sequence in which they appear in the SRG.)

We will also examine how a real Mobile Device Management platform can address these requirements. The examples will be taken from MobileFirst Protect Devices, an MDM system currently in use at numerous federal agencies.

About IBM® MobileFirst® Protect

A few facts about MobileFirst Protect:

- The first MDM solution to receive an authority to operate (ATO) in accordance with the US Federal Information Security Management Act (FISMA).[3]
- Selected as Best Security Solution by the Government Technology Research Alliance (GTRA) in December 2011.[4]
- Won the Best Enterprise Mobile Service award at Mobile World Congress 2012.[5]
- Selected for Government-Wide Federal Enterprise Mobility Management Program - 7/11/2013.[6]
- 2015 Gartner Magic Quadrant for Enterprise Mobility Management Suites; IBM Named EMM Leader Again.[7]
- Received an “Outstanding” product viability assessment in the Gartner Critical Capabilities for Mobile Device Management research report of August 2012, as well as receiving the first or second highest rating for “As-a-service and cloud delivery models,” “Agile Deployments,” “Mass Deployments,” and “Overall Score in Use Cases.”[8]

2012 Telework Exchange Tele-Vision Award for Innovative Technology to Support Telework: US General Services Administration, Office of the CIO, A3 Program

“The US General Services Administration (GSA) established the A3 (Any Device, Anywhere, Anytime) Strategy to improve its organizational mobility. The initiative allows the agency to migrate to a mobile information technology solution, freeing employees to telework by replacing desktop computers with portable devices, including laptops, smartphones, and tablets…

The A3 Strategy has enabled GSA to offer its workforce a landmark telework agreement that serves as a teleworking blueprint for the entire Federal government. The revised GSA approach… creates a secure telework solution that reduces overhead costs–benefiting everyone from government IT managers to agency employees and taxpayers...Upon rollout to other government agencies, the anticipated return on investment is expected to be measured in billions of dollars.

GSA has become a flagship agency for telework vision through the deployment of its A3 Strategy. The biggest end-user impact is the ability to use any mobile device of their choosing… The objective is to enable effective customer service that delivers employees with seamless, trusted access to GSA-approved applications from any mobile device. **To do this, GSA employed the MobileFirst Protect Devices platform to secure, manage, track inventory, and monitor devices from a cloud-based console. In this instance, GSA found the MobileFirst Protect Devices platform met the critical needs for each device, including patching software for laptops and safeguarding smartphones and tablets that can easily be lost or stolen.”** https://www.teleworkexchange.com/events/tele-vision-award/events-detail/1436

Managing policies

Requirements from the MDM SRG

The MDM server must have the administrative functionality to centrally manage configuration settings, including security policies, on managed mobile devices. Rule ID: SRG-APP-000135-MDM- 000087-MDM_rule

The MDM server must have the administrative functionality to centrally manage the following security policy rule on managed mobile devices:

Enable or disable Bluetooth. SRG-APP-000135-MDM-000099-MDM_rule

Enable or disable Wi-Fi. SRG-APP-000135-MDM-000107-MDM_rule

Enable or disable the GPS receiver. SRG-APP-000135-MDM-000110-MDM_rule

Enable or disable all cameras. SRG-APP-000135-MDM-000112-MDM_rule

Enable or disable the USB Port mass storage mode. SRG-APP-000135-MDM-000121-MDM_rule

Enable or disable Wi-Fi tethering. SRG-APP-000135-MDM-000122-MDM_rule

The MDM server must notify when it detects unauthorized changes to the security configuration of managed mobile devices. SRG-APP-000286-MDM-000163-MDM_rule

The MDM server must be able to detect if the security policy has been modified, disabled, or bypassed on managed mobile devices. SRG-APP-000137-MDM-000151-MDM_rule

The MDM server must support the capability to deploy operating system and application updates via over-the-air (OTA) provisioning for managed mobile devices. SRG-APP-000128-MDM-000084-MAM_rule

The MDM server must produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format. SRG-APP-000088-MDM-000276-SRV_rule

The MDM server must record an event in audit log each time the server makes a security relevant configuration change on a managed mobile device. SRG-APP-000130-MDM-000272-SRV_rule

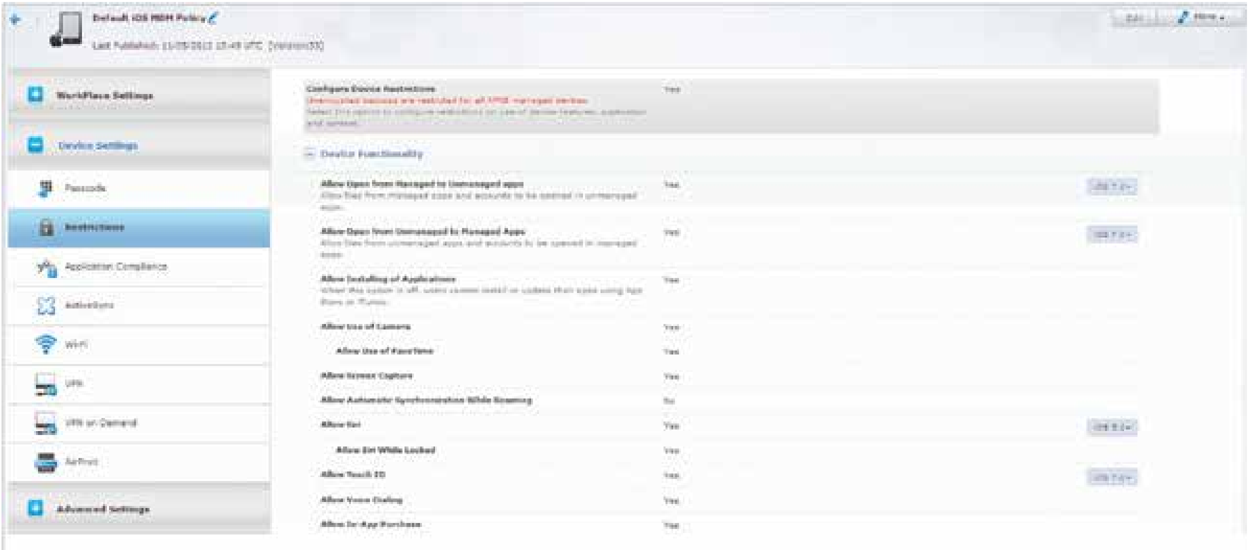
How MobileFirst Protect Devices can help

Note: Although the SRG uses the term "MDM Server," cloud-based solutions can accomplish the same requirements without requiring a server in the data center. They can also help agencies achieve the goals of the Office of Management and Budget's "Cloud First" policy (without the risks entailed in storing application data in the cloud).

Set security policies and push them to mobile devices

The MobileFirst Protect Devices platform helps administrators enable or disable hardware and software features, including:

- Cameras
- USB connections
- Bluetooth
- Wi-Fi tethering
- Data networks (such as Wi-Fi)
- GPS for location detection
- Native web browsers
- Email clients



Default iOS MDM Policy
Last Published: 11/05/2013 15:49 UTC (Version33)

Configure Device Restrictions — Yes
Unencrypted backups are restricted for all MDM managed devices
Select this option to configure restrictions on use of device features, application and content.

Device Functionality

Allow Open from Managed to Unmanaged apps — Yes
Allow files from managed apps and accounts to be opened in unmanaged apps.

Allow Open from Unmanaged to Managed Apps — Yes
Allow files from unmanaged apps and accounts to be opened in managed apps.

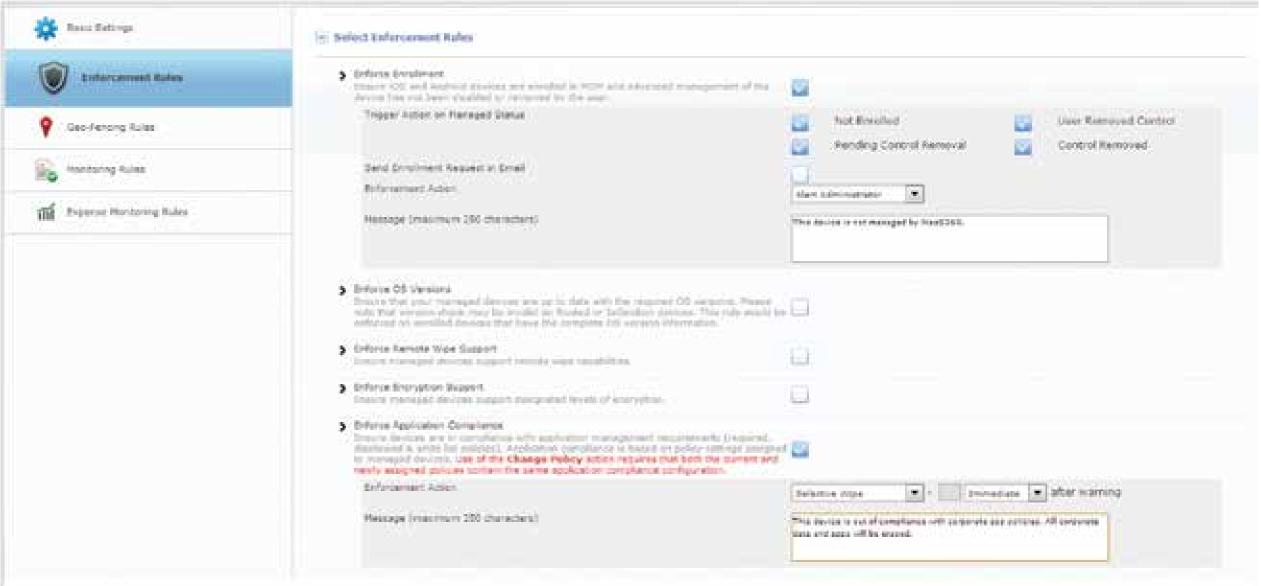
Allow Installing of Applications — Yes
When this option is off, users cannot install or update their apps using App Store or iTunes.

Allow Use of Camera — Yes
Allow Use of FaceTime — Yes
Allow Screen Capture — Yes
Allow Automatic Synchronization While Roaming — No
Allow Siri — Yes
Allow Siri While Locked — Yes
Allow Touch ID — Yes
Allow Voice Dialing — Yes
Allow In-App Purchase — Yes

Figure 1: Administrators can enable or disable a wide range of hardware and software features on mobile devices

As illustrated in *Figure 1*, for many of these, the administrator can choose between enabling, disabling, and letting users decide whether to enable the feature.

Many OS-specific features can also be controlled. For example, administrators can disable Siri and iCloud backup on Apple iOS devices.



Select Enforcement Rules

Enforce Enrollment ☑
Ensure iOS and Android devices are enrolled in MDM and advanced management of the device has not been disabled or removed by the user.

Trigger Action on Managed Status: ☑ Not Enrolled ☑ User Removed Control ☑ Pending Control Removal ☑ Control Removed
Send Enrollment Request in Email: □
Enforcement Action: Alert Administrator
Message (maximum 250 characters): This device is not managed by MaaS360.

Enforce OS Versions □
Ensure that your managed devices are up to date with the required OS versions. Please note that version check may be invalid on Rooted or Jailbroken devices. This rule would be enforced on enrolled devices that have the complete OS version information.

Enforce Remote Wipe Support □
Ensure managed devices support remote wipe capabilities.

Enforce Encryption Support □
Ensure managed devices support designated levels of encryption.

Enforce Application Compliance ☑
Ensure devices are in compliance with application management requirements (required, disallowed & white list policies). Application compliance is based on policy settings assigned to managed devices. Use of the Change Policy action requires that both the current and newly assigned policies contain the same application compliance configuration.

Enforcement Action: Selective Wipe - Immediate after warning
Message (maximum 250 characters): This device is out of compliance with corporate app policies. All corporate data and apps will be erased.

Figure 2: MobileFirst Protect Devices can detect when a device is out of compliance with policies, and then respond with a variety of defensive actions

Detect modifications and block devices that are out of compliance

MobileFirst Protect Devices features a Compliance Engine that lets IT administrators easily define and implement compliance rules for smartphones and tablets to deal with specific events and contextual changes. Managed devices are continuously monitored for violations of defined rules or events. Policies and events that can be monitored include minimum operating system version, encryption enforced, application white lists and black lists, SIM change, roaming state change, and jailbreak/root detection. (*Figure 2*)

If a policy violation occurs, MobileFirst Protect Devices can take action by:

- Alerting the user and administrator
- Blocking corporate email access
- Preventing the device from using Wi-Fi and VPN connections
- Wiping the device's memory to factory default settings

OTA provisioning and update

MobileFirst Protect Devices provides the ability to provision and update mobile devices over-the-air (OTA). It can enforce minimum operating system versions, “push” Wi-Fi, VPN and email clients, push content like documents and spreadsheets, push required security applications, and give users access to approved app stores.

MobileFirst Protect Devices also provides flexible provisioning procedures:

- Mobile devices can be provisioned directly by administrators
- Administrators can send users an enrollment request by email and SMS
- Authorized users can enroll and provision their own devices through a self-service portal

Audit trails

MobileFirst Protect Devices creates a centralized audit trail of the operational and security events on each mobile device. Administrators can analyze the log data to track configuration changes, as well as events that may indicate an attack or security violation.

Communications and storage

Requirements from the MDM SRG

The MDM server must use cryptography to protect the integrity of remote access sessions with managed mobile devices. SRG-APP-000015-MDM-000165-MDM_rule

The cryptographic module supporting encryption of data in transit (including email and attachments) must be FIPS 140-2 validated. SRG-APP-000197-MDM-000159-MDM_rule

The MDM server must encrypt all data in transit (e.g., mobile device encryption keys, server PKI certificates, mobile device data bases) using AES encryption (AES 128-bit encryption key length is the minimum requirement; AES 256 desired). SRG-APP-000264-MDM-000224-SRV_rule

The MDM server must employ automated mechanisms to facilitate the monitoring and control of remote access methods. SRG-APP-000016-MDM-000016-SRV_rule

The MDM server must provide the administrative functionality to transmit a remote Data Wipe command to a managed mobile device. SRG-APP-000135-MDM-000086-MDM_rule

The MDM server must have the administrative functionality to perform a “Data Wipe” function whereby all data stored in user addressable memory on the mobile device and the removable memory card is erased when the maximum number of incorrect passwords for device unlock has been reached. SRG-APP-000135-MDM-000088-MDM_rule

How MobileFirst Protect Devices can help

Encryption

MobileFirst Protect Devices allows administrators to require that data stored on devices be encrypted.

In addition, the information communicated between mobile devices and MobileFirst Protect Devices is transmitted over the SSL 3.0/TLS 1.0 protocol, using FIPS 140-2 compliant encryption modules.

Monitoring remote access methods

MobileFirst Protect Devices can also monitor and control remote access methods, for example by distributing VPN (Virtual Private Network) profiles, enforcing the use of VPNs for remote communications, and tracking the use of remote data networks, and allowing or disallowing the use of Wi-Fi connections.

Wiping devices

MobileFirst Protect Devices also allows administrators to perform both “full” and “selective” data wipes. The former removes all data from the device, but the latter removes just enterprise data and applications, leaving behind the user’s personal information and applications.

The system also has features to protect users from unnecessary wipes, for example by sending messages warning that a wipe will be performed after a grace period if the user does not take action to bring the device back into compliance.

User and device authentication

Requirements from the MDM SRG

The MDM server must uniquely identify mobile devices managed by the server prior to connecting to the device. SRG-APP-000158-MDM-000153-MDM_rule

The MDM server must disable network access by unauthorized server components or notify designated organizational officials. SRG-APP-000228-MDM-000030-SRV_rule

The MDM server must provide mutual authentication between the MDM server and the provisioned device during a trusted over-the-air (OTA) provisioning session. SRG-APP-000128-MDM-000083- MDM_rule

The MDM server must have the capability to enable and disable a managed mobile device. SRGAPP- 000134-MDM-000166-MDM_rule

The MDM server must have the administrative functionality to centrally manage the following security policy rule on managed mobile devices:

Enable or disable device unlock password. SRG-APP-000135-MDM-000091-MDM_rule

Maximum password age (e.g., 30 days, 90 days, 180 days). SRG-APP-000135-MDM-000092-MDM_rule

Set the number of incorrect password attempts before a data wipe procedure is initiated (minimum requirement is 3-10). SRG-APP-000135-MDM-000132-MDM_rule

How MobileFirst Protect Devices can help

Access control

MobileFirst Protect Devices can block unauthorized devices from accessing the enterprise network. It also has the ability to “quarantine” unknown devices; that is, to block the devices from the enterprise network until an administrator can review them and make a decision about whether to provide access.

Managed devices can be disabled by the administrator if they are out of compliance, or if there is a suspicion that the device has been lost or stolen.

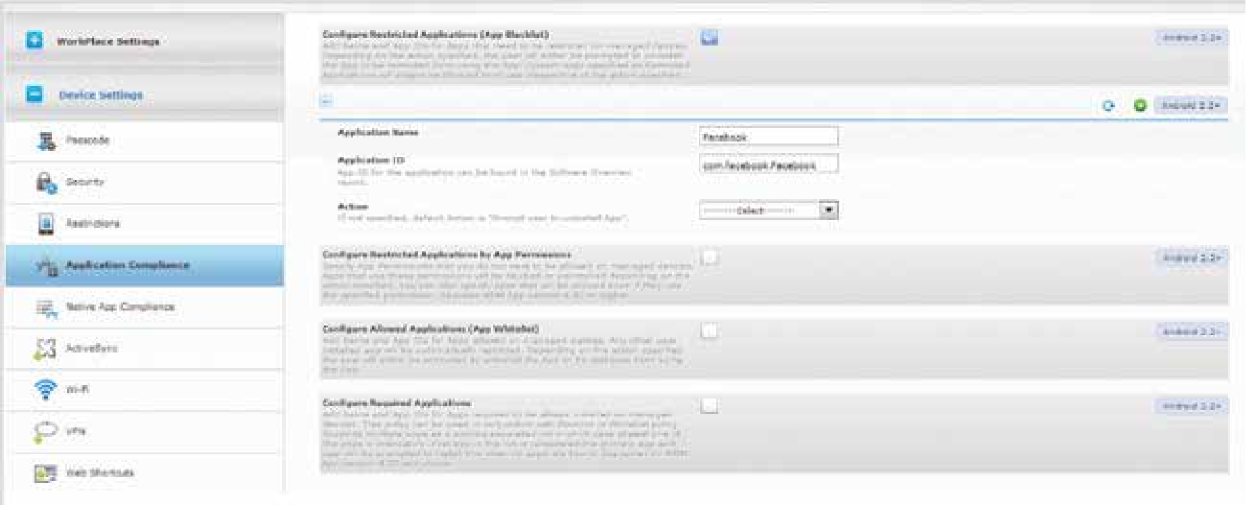
Authenticating devices to the server

MobileFirst Protect Devices uses digital certificates to authenticate mobile devices to the MobileFirst Protect server.

For example, Apple iOS devices use the Simple Certificate Enrollment Protocol (SCEP) to generate a certificate enrollment request for the MobileFirst Protect Certificate Authority (CA), which sends the device an identity certificate. For Android devices, the MobileFirst Protect Devices platform sends encrypted configuration information over the air.

Managing passwords

MobileFirst Protect Devices allows administrators to control password policies on mobile devices. For example, rules can be established about whether passwords need to include a letter, the minimum password length, the maximum allowable age for passwords, the idle time allowed before the device is locked and needs to be opened again with a password, and the number of failed login attempts that are allowed before data on the device is wiped. *Figure 3* shows the password policies available for iOS devices (note that the password policies supported varies between different mobile device platforms). Administrators can also reset passwords on mobile devices remotely.



Configure Restricted Applications (App Blacklist)

Application Name: Facebook

Application ID: com.facebook.Facebook

Action: --------Select--------

Configure Restricted Applications by App Permissions

Configure Allowed Applications (App Whitelist)

Configure Required Applications

Figure 3: MobileFirst Protect Devices lets administrators create strong password policies for mobile devices

Applications

Requirements from the MDM SRG

The MDM server must detect and report the version of the operating system, device drivers, and application software for managed mobile devices. SRG-APP-000270- MDM-000162-MDM_rule

The MDM server must support organizational requirements to install software updates automatically on managed mobile devices. SRG-APP-000269-MDM- 000161-MAM_rule

The MDM server device integrity validation component must use automated mechanisms to alert security personnel when the device has been jailbroken or rooted. SRG-APP-000237-MDM-000175-MDIS_rule

The MDM server must have the administrative functionality to centrally manage the following security policy rule on managed mobile devices:

Enable or disable the mobile device user's access to an application store or repository. SRG-APP-000135-MDM-000115-MDM_rule

Prohibit the mobile device user from installing unapproved applications. SRG-APP-000135-MDM-000148-MDM_rule

Prohibit the download of software from a DoD non-approved source (e.g., DoD operated mobile device application store or MDM server). SRG-APP-000135-MDM-000149-MDM_rule

Specify a list of approved applications that must be installed on the mobile device and cannot be removed by the user. SRG-APP-000135-MDM-000150-MDM_rule

How MobileFirst Protect can help

Hardware and software inventory

MobileFirst Protect begins by providing a detailed hardware and software inventory of devices, including reports for each device about the processor, RAM, internal and external storage, battery level, operating system version, firmware, and apps installed.

Jailbroken, rooted and out-of-compliance devices

Security-related information in the same reports includes if the device has been jailbroken or rooted, whether it is in or out of compliance with security policies, and the date of the last selective wipe.

Whitelists, blacklists and required applications

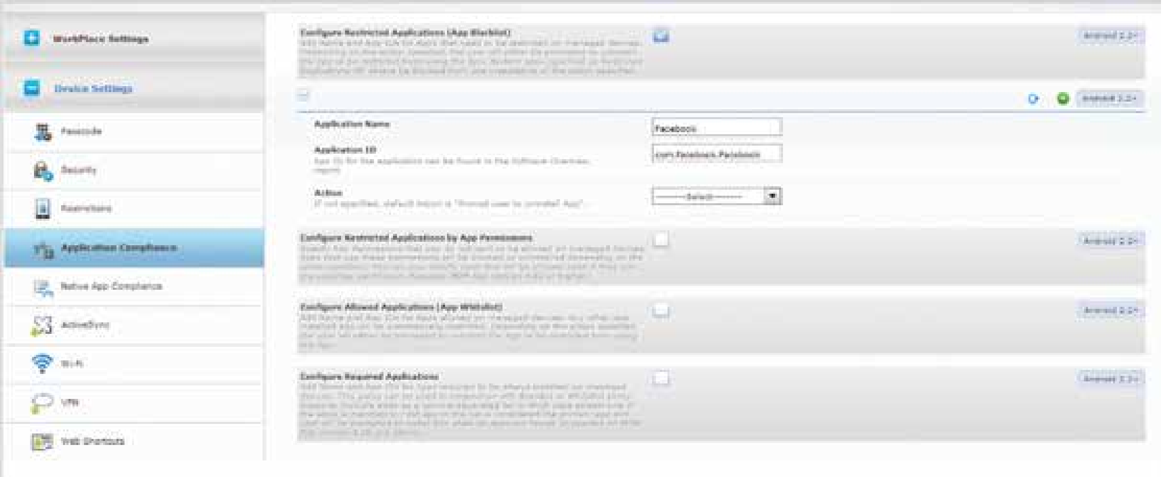
MobileFirst Protect Devices lets administrators set up application whitelists to allow specific applications to be installed on devices, blacklists to prevent applications from being installed or used, and event to require that specific applications be installed on the devices (*Figure 4*).

App store integration

Users can be guided to iTunes®, Google Play™ (for Android devices), Windows 7 Marketplace, and other authorized application sources. Alternately, MobileFirst Protect Devices can restrict downloads to an approved enterprise app store, or narrow app sourcing even further by creating an app catalog customized for each user based on his or her group, operational unit, or individual authorization.

Updating apps

MobileFirst Protect Devices includes a set of workflows for managing the lifecycle of mobile apps. These address collecting software inventory, tracking app distribution and installation, and publishing app updates.



Configure Restricted Applications (App Blacklist) ☑

Application Name: Facebook

Application ID: com.facebook.Facebook

Action: ---------Select---------

Configure Restricted Applications by App Permissions □

Configure Allowed Applications (App Whitelist) □

Configure Required Applications □

Figure 4: MobileFirst Protect Devices lets administrators create app blacklists, whitelists, and required app lists

Additional capabilities for MDM platforms

The two documents we have been discussing, the *NIST Guidelines for Managing and Securing Mobile Devices* in the *Enterprise and the DOD Mobile Device Management (MDM) Server Security Requirements Guide*, are focused primarily on features that affect information security. But there are capabilities unrelated to security that are also very important. We list just a few of them here.

Expense monitoring

An MDM system can be used to monitor and control telecom expenses. For example, users and administrators can be alerted when roaming usage reaches predefined levels. This can prevent mobile users from inadvertently exceeding the telecom budget. Other measurements help administrators and managers predict and control costs. (*Figure 5*)

Content management

Administrators can push content such as word processing and pdf documents, spreadsheets, and presentations, to individuals or groups of smart devices through the MobileFirst Protect Content. A policy can be set so that the content can be viewed, but not deleted or moved out of the MobileFirst Protect container. Timers can be set to automatically remove content from a smart device after a certain period of time.

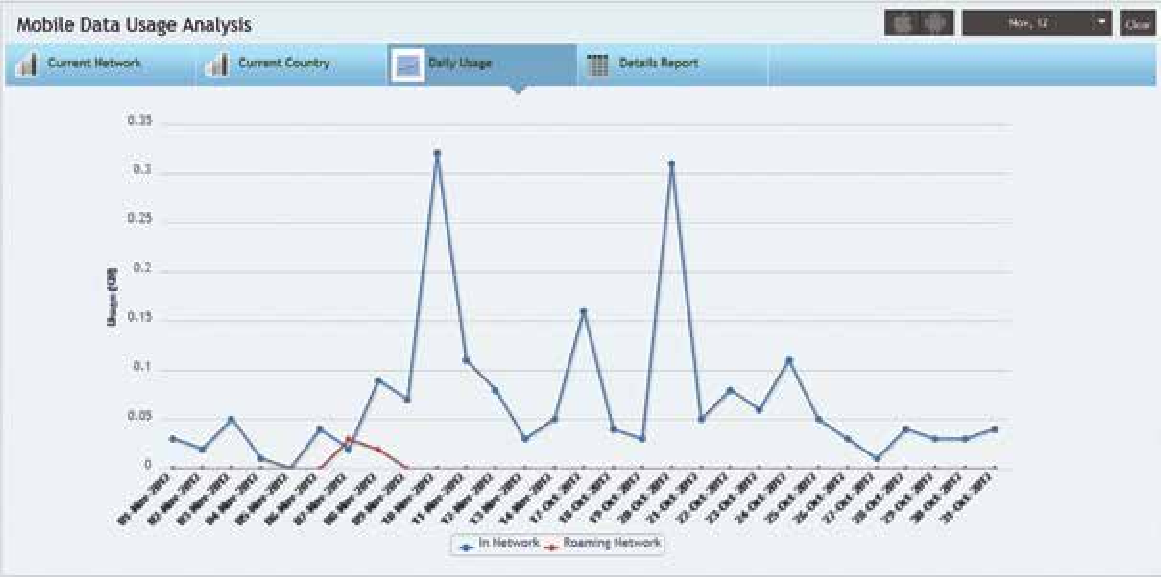


Figure 5: An MDM system can help monitor and control telecom costs

Metrics and reporting

An MDM platform can gather data from hundreds or thousands of mobile devices and incorporate them into metrics and reports related to security and operations. These metrics and reports can be used to troubleshoot issues, anticipate problems and track trends. *Figure 6* is an example of a report that shows "at a glance" the number of smartphones and tablets being monitored, by operating system.

MobileFirst Protect Devices can also provide sanitized best practice data from a cross section of groups within the organization, so groups can measure themselves against their peers.

Personal privacy protection

MobileFirst Protect Devices includes a policy setting to mask at the console the personal apps and location services on a device. This provides a degree of anonymity for devices when there is no "need to know," or when it is necessary to protect the privacy of personal devices in organizations with a "Bring Your Own Device" option for employees.

Unified platform for laptops and smartphones

The NIST and DOD documents we have been discussing explicitly limit themselves to smartphones and mobile devices, but other publications cover the central management of laptops and notebooks. A very small number of products provide a unified platform for managing laptops and smartphones together. A unified platform simplifies management, displays the mobile needs and activities of users, lowers operating costs, and meets the new OMB Digital Government requirements for utilizing Shared Services.[9]

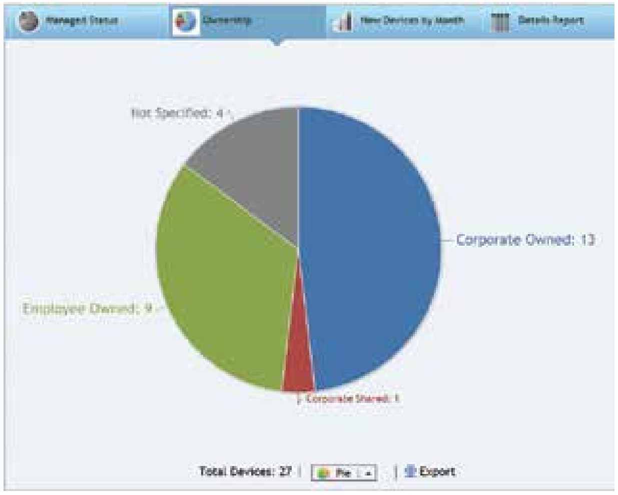


Figure 6: Metrics and reports can help managers troubleshoot issues, anticipate problems and track trends

Cloud-based for fast adaptation and scaling

In a world of advanced persistent threats and zero-day attacks, fast reaction and adaptation can mean the difference between good security and a breach.

A cloud-based MDM platform has major advantages over an MDM product running on an appliance, or hosted in a server in a third-party data center. That is because the cloud solution provider can make features available automatically to customers when a new device is introduced, or an operating system is upgraded, or a new threat is identified. Enterprises do not need to roll out patches to their appliances or servers, or submit change control requests to the vendor, or upgrade MDM hardware and software before they can use new features and protect additional users.

For example, MobileFirst Protect Devices was able to provide new policy options for Android Jelly Bean and Apple iOS 6 devices on the same day that the operating systems went into general release.

Summary

Mobile Device Management is a complex subject. But the NIST *Guidelines* document and the DISA MDM SRG, although still evolving, are already valuable resources for coming up to speed on possible requirements for MDM systems.

The requirements can be grouped into four categories:
1. Managing policies
2. Data communication and storage
3. User and device authentication
4. Applications

An advanced Mobile Device Management platform can address many of these requirements by helping administrators and managers perform the following:

- Set security policies and push them to the devices
- Detect modifications to security parameters on devices and block devices that are out of compliance from accessing the enterprise network
- Provision and update devices over-the-air (OTA)
- Collect and compile audit trails from thousands of mobile devices
- Enforce the encryption of "data at rest" and "data in motion"
- Monitor remote access methods
- Wipe devices that are lost and stolen to remove all enterprise data
- Enforce access control on devices
- Authenticate devices to the server
- Manage passwords
- Collect and compile hardware and software inventory information
- Identify jailbroken, rooted and out-of-compliance devices and prevent them from accessing the enterprise network
- Manage and enforce application whitelists, blacklists and lists of required applications
- Provide integration with public and private app stores
- Update mobile operating systems and apps over the air
- Monitor telecom expenses
- Distribute and control documents and files (Content Management)
- Provide detailed metrics and reporting
- Manage laptops and notebooks as well as smartphones

Finally, cloud-based MDM platforms like MobileFirst Protect Devices can make features available automatically to customers, so enterprises can feel confident about rolling out patches or managing server hardware and software.

Start using MobileFirst Protect mobile device, application, document and expense management today – at no cost! Go to ibm.biz/mobilefirst-protect.

About IBM MobileFirst

IBM's 6,000 mobile experts have been at the forefront of mobile enterprise innovation. IBM has secured more than 4,300 patents in mobile, social and security, which have been incorporated into IBM MobileFirst solutions that enable enterprise clients to radically streamline and accelerate mobile adoption, help organizations engage more people and capture new markets. Through IBM's partnership with Apple, the two organizations are transforming enterprise mobility with a new class of industry specific business apps. For more information on IBM MobileFirst, visit www.ibm.com/mobilefirst. To learn more about IBM MobileFirst Protect and start a no cost 30-day trial, visit ibm.biz/mobilefirst-protect.

Why IBM?

IBM Security solutions are trusted by organizations worldwide for fraud prevention and identity and access management. The proven technologies enable organizations to protect their customers, employees, and business-critical resources from the latest security threats. As new threats emerge, IBM can help organizations build on their core security infrastructure with a full portfolio of products, services and business partner solutions. IBM empowers organizations to reduce their security vulnerabilities and focus on the success of their strategic initiatives. To learn more about IBM Security fraud-prevention solutions, please contact your IBM representative or IBM Business Partner, or visit the following website: ibm.com/security

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM® X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents. Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: ibm.com/financing

[1] Murugiah, S. and Scarfone, K.; NIST Special Publication 800-124 Revision 1 (Draft), *Guidelines for Managing and Securing Mobile Devices in the Enterprise.* Section 2.2 is on pages 3-6; National Institute of Standards and Technology, U.S. Department of Commerce; July 10, 2012; available at http://csrc.nist.gov/publications/drafts/800-124r1/draft_sp800-124-rev1.pdf.

[2] *The Mobile Device Management (MDM) Server Security Requirements Guide* (Draft) Version: 1, Release 0.2, 18 July 2012, together with an overview memo, is available in a zipped file at: http://csrc.nist.gov/publications/PubsSPs.html#800-124 (Hit CTRL + F then type in "SP 800-124 Rev. 1"). The SRG document is in XML format.

[3] IBM Security Solutions; *MaaS360 First to Receive Federal Government Authority to Operate Mobile Device Management*; Press Release; 9/28/2011; http://www.maas360.com/news/press-releases/2011/maas360-first-to-receive-federal-government-authority-to-operate-mobile-device-management/

[4] IBM Security Solutions; *Government Technology Officials Name MaaS360 Best Security Solution;* 12/13/2011; Press Release; http://www.maas360.com/news/press-releases/2011/government-technology-officials- name-maas360-best-security-solution/

[5] IBM Security Solutions; *MaaS360 Wins Best Enterprise Mobile Service at Mobile World Congress;* Press Release; 2/29/2012; http://www.maas360.com/news/press-releases/2012/maas360-wins-best-enterprise-mobile-service-at-mobile-world-congress/

[6] IBM Security Solutions; *MaaS360 Selected for Government-Wide Federal Enterprise Mobility Management Program;* 7/11/2013; Press Release; http://www.maas360.com/news/press-releases/2013/maas360-selected-for-government-wide-federal-enterprise-mobility-management-program/

[7] IBM Security Solutions; *2015 Gartner Magic Quadrant for Enterprise Mobility Management Suites; IBM Named EMM Leader Again;* Analyst Report; 6/8/2015; https://www.maas360.com/lp/ar-2015-gartner-magic-quadrant/

[8] IBM Security Solutions; *Fiberlink Achieves "Outstanding" Product Viability Score in Report on Critical Capabilities for Mobile Device Management;* Press Release; 7/31/2012; http://www.maas360.com/news/press-releases/2012/fiberlink-achieves-outstanding-product-viability-score-in-report-on-critical-capabilities-for-mobile-device-management/

[9] OMB Reports: *OMB Digital Management Strategy; Building a 21st Century Platform to Better Serve the American People;* 2011; https://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
December 2015

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.

♲ Please Recycle