XenMobile Security Overview

Understanding the technology used by XenMobile to deliver comprehensive, end-to-end security.
Contents

Introduction
  The Evolution of Mobile Management
  Citrix Mobility Solution - XenMobile

XenMobile Server
  XenMobile Mobile Device Management (MDM)
  XenMobile Mobile Application Management (MAM)
  XenMobile Standalone MAM (MAM-Only)

XenMobile Architecture
  Secure Hub
  NetScaler Gateway

XenMobile Security Details
  Application Authentication Controls
  XenMobile Encryption
  FIPS 140-2 Compliance

How is My Data Protected at Rest?
  Secret Vault
  Kill Pill

How is My Data Protected in Transit?
  MicroVPN
  Encryption Level for TLS Session

How is My Data Protected Inside the Company?
  Internal Controls
  NetScaler
  XenMobile Server
  XenMobile Apps
  Citrix Receiver
  Cryptography
  Device/Server Verification

Operational Security Features
  Enrollment
  Initial Enrollment Flow Diagrams
  Remote Data Wipe
  Application Execution Prevention
  Web Services
  Automated Actions
  Auditing Capability
  Ensuring Denial of Service Protection
  PKI Integration and Distribution

Summary

References and Appendices
  XenMobile MDX-Enabled Applications
  Logical Component Diagram
  About the Authors and Contributors
Introduction
Mobility initiatives are a top priority for IT organizations. More employees than ever are demanding access to applications and data that help them achieve maximum productivity outside the office. But satisfying mobility requirements is becoming more challenging as employee expectations continue rising.

Today, employees want access to all their apps from any mobile device, including their own personal devices. Modern mobile apps have expanded beyond conventional tools and use cases, such as mobile email. They now include Windows, web and native mobile apps, delivered both from the cloud as well as the company datacenter. These apps are also being distributed broadly across different locations and mobile end points.

Allowing users to access all their apps and data from untrusted devices and unpredictable locations raises significant security concerns for IT. The Citrix Secure Digital Workspace offers the most complete and integrated solution to enable people to securely access their apps, desktops and data from anywhere. And only a Citrix Workspace offers you complete choice of device, cloud and network, streamlined for IT control and simple, secure access for users. XenMobile is the cornerstone of mobility management in the Citrix Secure Digital Workspace. This white paper will help mobile technologists understand critical mobility requirements with respect to security. It also explains the technology used by XenMobile to deliver comprehensive, end-to-end mobile protection.

The Evolution of Mobile Management
Enterprises initially turned to Mobile Device Management (MDM) solutions to manage their devices. MDM not only centralized device management, it also gave IT the ability to perform remote configurations and updates, and easily deliver applications and data to mobile end points. MDM helped IT organizations overcome early bring-your-own-device (BYOD) challenges, such as onboarding and large-scale management.
**Mobile Application Management (MAM)** emerged soon after MDM and focuses on securing and managing applications as individual components. MAM offers a similar set of policies and user experience management as MDM, but at an individual application level rather than the device level. Since then, MAM has expanded to encompass app-level control of secured “micro-VPNs,” inter-container communication, and encrypted sandbox containers.

MAM has also gained in popularity as a standalone (MAM-only) alternative to MDM for enterprises that want to roll out **Bring Your Own Device (BYOD)** policies. Employees are becoming increasingly resistant to enrolling in corporate MDM user privacy concerns and putting their personal information at risk to an accidental or deliberate wipe by IT.

**Enterprise Mobility Management (EMM)**, an approach that combines MDM, MAM and Mobile Content Management (MCM). EMM is the key to managing personal devices in a corporate setting at scale – without impacting user experience, and without inflating costs or introducing security risks.

Most recently, **Unified Endpoint Management (UEM)** has emerged as an approach to securing and controlling desktop computers, laptops, smartphones and tablets, in a connected, cohesive manner from a single console. Unified endpoint management typically relies on the mobile device management (MDM) application program interfaces (APIs) in desktop and mobile operating systems.

Of course, an EMM/UEM solution alone is not enough to ensure the success of mobile initiatives. IT organizations still need the right network infrastructure in place to ensure that applications and data are delivered across different devices securely, while also addressing performance, management and scale requirements. This includes protecting data on-premises, in transit and on mobile devices.

Common network infrastructure components and management tools used for mobile initiatives include:
- Firewalls
- VPNs
- Wi-Fi networks
- Application management/push technology
- Monitoring products
- Intrusion Detection System
- Workflow automation
- System imaging technology
- Policy management
An EMM/UEM solution also benefits from the evaluation of business needs, user needs and work/life considerations. Many organizations are using their mobile initiatives to re-think the way they provide all IT services to end-users. They are now implementing public/private clouds, application/desktop virtualization, application layer firewalls/network gateways, security assertion markup language (SAML), and certificate services to assist and secure service delivery.

“According to a recent Ponemon study sponsored by Citrix, the protection of apps and data is more critical than ever, with 74 percent of businesses saying that a new IT security framework is needed to improve security posture and reduce risk.”


Enterprise Mobility Management (EMM)/ Unified Endpoint Management (UEM) functionality of the Citrix Secure Digital Workspace is an important component of a reasonable General Data Protection Regulation (GDPR) compliance program:

1. The Citrix Workspace allows enterprises to establish a clear boundary between personal and business data on the device. IT doesn’t have access to the content of personal apps or personal email accounts on the device. This is critical to the data minimization as well as the integrity and confidentiality principle of GDPR.

2. The Citrix Workspace gives IT visibility into which devices and apps are accessing business services. In the case of a data breach, the IT administrator can show through audit logging exactly what actions took place leading up to the compromise and what, if any, actions IT took as a result. This provides a clear record of any unauthorized access to business services and supports the GDPR principle of integrity and confidentiality, as well as of accountability. Citrix’s solution enables IT to:
   a. Manage inventory
      i. Identify authorized and unauthorized devices.
      ii. Identify authorized and unauthorized apps.
   b. Whitelist applications
      i. Establish a subset of applications that are authorized to run on a device and access business services.
   c. Protect Access
      a. Allow only authorized users, devices, and apps to access business services, whether on-premises or in the cloud.
   d. Provide audit logging
      i. Monitor administrative actions and business data flows.
3. The Citrix Workspace allows the IT administrator to protect the device from security threats, which is important for the principle of integrity and confidentiality, as well as of accountability. Citrix’s solution enables the IT administrator to enforce compliance:
   a. Apply appropriate security configurations and policies to the devices and applications.
   b. Actively Monitor the security compliance of the device and applications, including attacks on the integrity of the operating system to jailbreak or root the device.
   c. Take remediation actions if the device or application is out of compliance via automated actions.

For additional information on what GDPR is and how to make your ready reference: https://www.citrix.com/blogs/2017/06/08/you-can’t-touch-this/

Citrix Mobility Solution - XenMobile

**Citrix® XenMobile®** provides comprehensive, end-to-end security, and delivers the full breadth of EMM capabilities along with an engaging user experience.

In fact, only Citrix delivers a single integrated EMM solution to manage mobile devices as well as mobile apps, web apps, desktops and desktop applications. This integrated approach helps IT further reduce costs by leveraging the same architecture, hardware and devices for end-to-end application and data delivery. XenMobile facilitates positive user experiences that improve productivity and help eliminate shadow IT while ensuring employee privacy and providing enterprise-grade protection for corporate data and assets.

XenMobile leverages the enterprise-proven knowledge and technologies of Citrix to provide a complete, integrated and scalable solution for delivering apps and data to any device while maintaining security and a high-performance end user experience from any location.

<table>
<thead>
<tr>
<th>Security Feature</th>
<th>XenMobile</th>
<th>Competition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using Inbuilt CA or third-party PKI’s Certificates to establish trust during enrollment</td>
<td>Yes</td>
<td>Limited</td>
</tr>
<tr>
<td>Certificate Pinning to prevent (Man in The Middle) attacks</td>
<td>Yes</td>
<td>Limited</td>
</tr>
<tr>
<td>MicroVPN Communication between the device and the MDM gateway server</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Uses own encryption vault instead of leveraging iOS key chain</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Purpose built Linux based appliance for MDM/MAM server</td>
<td>Yes</td>
<td>Limited</td>
</tr>
<tr>
<td>Data Encryption for MDM server file system and clustered-shared database</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>SmartAccess for Mobile devices connecting to company resources</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

In the sections that follow, we’ll discuss XenMobile’s key components that enable security without compromising the user experience.
XenMobile Server

XenMobile Server is the central hub for XenMobile and enables both mobile device management (MDM) and mobile application management (MAM) through a single virtual Linux appliance. XenMobile Server offers a single console for management of devices, apps, and data. Whether, the deployment is on-premises or the XenMobile Service hosted in the Citrix Cloud a single code base is used for all implementations.

XenMobile Mobile Device Management (MDM)

XenMobile MDM allows you to manage mobile devices, set mobile policies and compliance rules, and gain visibility to the mobile network. It also provides control over mobile apps and data, and shields your internal network from mobile threats. With a “one-click” dashboard, simple administrative console, and real-time integration with Microsoft Active Directory, and other enterprise infrastructure such as public key infrastructure (PKI), and Security Information and Event Management (SIEM) systems, XenMobile Server simplifies the management of mobile devices.

<table>
<thead>
<tr>
<th>MDM device-level controls and visibility</th>
<th>MDM Console controls and visibility</th>
<th>MDM Server controls and visibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device-level password protection</td>
<td>Link to your Active Directory implementation for users and groups</td>
<td>Onboard mobile devices</td>
</tr>
<tr>
<td>Encryption</td>
<td>Enroll users and their devices with multi-factor security</td>
<td>Be certain your users are connecting to a valid XenMobile Server using Certificate Pinning</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Create and deploy policies</td>
<td>Automatically deploy device management configurations on the mobile device</td>
</tr>
<tr>
<td>Device inventory</td>
<td>Define and enforce compliance standards</td>
<td>Deploy packages for devices, users, and groups, with the ability to restrict deployment based on comprehensive rules and scheduling</td>
</tr>
<tr>
<td>Application inventory</td>
<td>View reports</td>
<td>Have visibility and auditing including user and device management configurations and settings, device hardware, software inventory, and connection logs</td>
</tr>
<tr>
<td>Selective/full device wipe</td>
<td>Set application blacklist and whitelists</td>
<td>Enable high availability and scalability through a multi-server redundant architecture and load balancing to support very large deployments</td>
</tr>
<tr>
<td>Specific device manufacturer APIs</td>
<td>Configure an email server</td>
<td>Take advantage of roles-based administration and delegation</td>
</tr>
<tr>
<td>Automated Configuration of Wi-Fi</td>
<td>Locate devices</td>
<td>Obtain online mobile activity reports, providing detailed information on users, devices, policies, and deployment packages</td>
</tr>
<tr>
<td>Restricted access to device resources: App Stores, camera, browser, etc.</td>
<td>Configure advanced PKI certificates or SAML authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Integrate with the Apple Device Enrollment Program</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configure Android for Work integration</td>
<td></td>
</tr>
</tbody>
</table>

XenMobile MDM can be used to manage iOS, Android, Windows Phone 8/10, and Windows Mobile. It can also, be used to manage Windows 8/10 and macOS desktops, laptops, and tablets.
XenMobile Mobile Application Management (MAM)

XenMobile provides the industry’s most comprehensive set of MAM capabilities to secure information at the application level. XenMobile MAM allows you to protect enterprise apps and data with policy-based controls, such as restricting access to authorized users, automatic account de-provisioning for terminated employees, and remote wipe for data and apps stored on lost devices.

With XenMobile MAM, you can provide the following benefits for each application type:

- Centralized user account creation and management for applications.
- The use of Active Directory as the identity repository and basis for authorizing users for external applications and services.
- A unified enterprise app store to enable the publishing and distribution of Android-, iOS-, and Windows Phone-based applications for authorized users to download and install on mobile devices.
- Access to virtual Windows applications and desktops with seamless SSO (no redundant prompts for credentials)
- Centralized policy controls to secure applications and data, with easy removal of user accounts, erase and lock of Citrix-delivered applications and data, and consolidated auditing and reporting of application access.

XenMobile MAM also includes the Citrix MDX app container technology:

- An additional layer of AES-256 encryption is provided for files and DBs on mobile devices. This is above and beyond what the device OS/hardware may or may not provide. It can be leveraged at compile time, or later via wrapping technology. All data stored by the application is placed in a secure container that encrypts both files and embedded SQL technology on the devices.
- Mobile applications can have their network access controls managed by the solution to ensure network connections are routed appropriately thru secure SSL channels (MicroVPN) based on application, domain name, etc.
- Isolation from other user owned apps on mobile devices is also provided. Each application may receive its own SSL encrypted tunnel that can only be leveraged by that application.
- Applications inherit all MDX security features, including SSO, secure inter-app communication, information/data containment, restrictions based on device states.

In addition, MDX provides a springboard to virtual apps and desktops from your mobile platform. VDI and virtual application capabilities for desktops are fully portable as part of the Citrix mobile platform. These apps can leverage the Citrix compile time embedded policies. They may alternatively accomplish the same objectives via wrapping after compile time. This will be discussed in more detail later. Additionally, there is a hybrid approach that includes public apps specifically programmed to leverage XenMobile application wrapping policies.
Per-Application Encryption and Policies
XenMobile allows administrators to include 60+ application-specific policies pre- and post-compile time. Administrators with access to source code can enhance their applications to include XenMobile security and policies by adding a single line of code to their application.

An application-wrapping tool is provided for applications where the source code cannot be accessed. This feature is supported on iOS and Android. Additionally, Citrix offers the XenMobile MDX Service available in Citrix Cloud. With the MDX Service, you can wrap iOS and Android apps from a browser on any OS. No initial setup is necessary, no need to install Android SDKs, no more trials-and-errors of setting up the correct paths, and no more importing of code signing certificates to macOS Keychain.

It should be noted that terms for the Apple store do not allow wrapping an application that has been signed and published to a public app store. Wrapping such applications requires approval by the respective developer(s). This produces challenges for IT, as there are a number of off-the-shelf applications that would be suitable for business use if they supported IT controls. For this reason, Citrix has partnered with many application developers to provide off-the-shelf, Citrix-enabled applications. There are hundreds of applications in Citrix Ready Marketplace – the marketplace for enterprise-ready mobile apps for XenMobile. No other vendor has this level of support and participation in their MAM arsenal.

Applications prepared at compile time or by using wrapping gain capabilities to enforce per-application encryption. This ensures that regardless of the encryption facilities provided by the OS, XenMobile applications are encrypted using AES-256 libraries. This includes local files and databases. Even if the device were to be jailbroken or rooted, the contents of these applications are protected.

Additionally, Administrators have options to enable offline access to applications and their respective data. When offline access is enabled, a strong cryptographic hash of the user password is stored on the device and is stored in the AES-256 encrypted container.

XenMobile Standalone MAM (MAM-Only)
Unlike most EMM solutions in the marketplace, XenMobile MAM provides all of the same security features and capabilities with or without MDM enrollment. This is becoming increasingly important as employees are becoming less and less likely to agree to MDM enrollment of their personally-owned devices.
XenMobile Architecture

Secure Hub
Secure Hub is the central control point on the mobile device for all XenMobile-wrapped or compiled applications as well as content stored on the device. Secure Hub manages the user experience springboard for authentication, applications, policy management and encryption variable storage. Once applications under management are started, they verify their policy status with the Secure Hub application.

NetScaler Gateway
NetScaler Gateway™ provides secure remote access from outside the corporate network while maintaining the highest level of protection for sensitive corporate data.

The key features of NetScaler Gateway are:
• FIPS-compliant appliance providing FIPS transport layer security (TLS) tunnel(s)
• Authentication
• Termination of encrypted sessions
• Access control (based on permissions)
• Data traffic relay (when the preceding three functions are met)
• Support for multiple virtual servers and policies

Authentication, Authorization, and Accounting
You can configure authentication, authorization, and accounting to allow users to log on to the NetScaler gateway with credentials that either Gateway or authentication servers located in the secure network, such as LDAP or RADIUS, recognize. Highly secured environments often augment LDAP/RADIUS with certificate-based authentication. Thus, a mobile device will perform dual-factor authentication while only requiring the user to enter a PIN/password. Authorization policies define user permissions, determining which resources a given user is authorized to access. Accounting servers maintain data about Gateway activity, including user logon events, resource access instances, and operational errors. This information is stored on Gateway or on an external server. NetScaler Gateway also allows you to create policies to configure how users log on. You can also restrict user logon by creating session and endpoint analysis policies.

Additional authentication methods include Azure Active Directory (AAD) and Derived Credentials.
XenMobile Security Details

Application Authentication Controls

Secure Hub serves as the encryption key broker for all MDX applications. Each application under management retrieves its policy check-in times from the Secure Hub application. The applications will then verify timers across each application/resource on the device.

When a user is successfully authenticated, an application specific token is generated with an associated expiration time applied. This key further encrypts and protects access to any user-based certificate delivered to the MDX framework.

This key is validated and stored in memory to encrypt / decrypt data for that specific application. When the key expires, the application will obtain a new key based on current authentication status and policy.

XenMobile Encryption

Each time the Secure Hub application connects to XenMobile Server a unique token is generated by Secure Hub and passed to the XenMobile services running on the XenMobile Server appliance.

XenMobile Server provides application management and policy control for MDX-secured applications. XenMobile Server validates this user/device from an asynchronous connection to the NetScaler to ensure the device is what it claims to be and that the NetScaler has successfully authenticated it.

XenMobile Server then generates strong cryptographic random numbers, which are then encrypted and sent via SSL tunnel back to the device.

Secure Hub leverages its unique token to decrypt the package and retrieve its unique cryptographic random numbers, which will be used in the generation of the AES keys for the device. Secure Hub protects these variables in its encrypted keychain for later use as needed. The server provides random numbers, the device ID, and other unique values that are used in the AES key generation.

Secure Hub utilizes these cryptographically strong variables to generate an AES encryption key. The encryption key on iOS and Android are both AES-256 bit keys. The resultant key is then used by MDX applications to encrypt all of their data prior to writing it to the device.

FIPS 140-2 Compliance (available on-premises only)

The Federal Information Processing Standard (FIPS), issued by the US National Institute of Standards and Technologies (NIST), specifies the security requirements for cryptographic modules used in security systems. FIPS 140-2 is the second version of this standard.

XenMobile release 10 has achieved broad end-to-end FIPS 140-2 compliance. Data-at-rest and transit cryptographic operations are using FIPS-certified cryptographic modules.
Device Data at Rest – At a Glance

<table>
<thead>
<tr>
<th>Platform</th>
<th>Location</th>
<th>Strength</th>
<th>Key Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS</td>
<td>MDX Applications</td>
<td>AES-256</td>
<td>Citrix Secret Vault</td>
</tr>
<tr>
<td>Android</td>
<td>MDX Applications</td>
<td>AES-256</td>
<td>Citrix Secret Vault</td>
</tr>
</tbody>
</table>

How Is My Data Protected at Rest?

Most employees today do their best to protect company interests. But the stress of work and the need for productivity can drive employees to make bad decisions. This situation often arises in the form of users leveraging applications and cloud storage systems that are not under company control, or who copy/paste sensitive content to unprotected email systems. These applications make the mobile end user experience more productive, but raise the risk of losing control of the data. At the opposite end of the spectrum are malicious users who may be attempting to steal company assets. Regardless of the motive, IT needs tools to protect company property.

Considerations:

- Control Copy/Paste: XenMobile MDX can prevent copy/paste or only allow it to happen across company-wrapped applications. Thus, a separation of company/private data is achieved.
- Restrict Open-In: Controls are provided so that opening documents can only be performed in company-wrapped applications. When an employee receives an email with an attachment, all personal apps on the device with the ability to open the document will be made unavailable. Only company-approved apps will be able to perform this function. Even links to web sites can be forced to open within a secure browser. (Administrators can set specific exceptions to this policy when needed, such as for Office 365 mobile applications.)
- Restrict Usage: Permit app usage only on the company network based on application-level policies (copy/paste/network access, etc.) and inter-app access controls (open-in, etc.).
Secret Vault

Secret Vault is supported across mobile platforms to address common security concerns with platform-native key stores such as iOS keychain. Secret Vault is a strong encryption layer that is used by Secure Hub and other XenMobile applications to persist their sensitive data, such as passwords and encryption keys on the device.

The Secret Vault can be used in 2 modes – one where the encryption key is stored on the device, and a more secure form where the encryption key is composed of user entropy data. User entropy is a user-generated random PIN code that only the user knows. The PIN adds an additional layer of security from hacking attempts. The PIN is never cached on the device.

XenMobile stores sensitive data in Secret Vault instead of platform-native stores such as the iOS keychain. The data persisted in Secret Vault include Active Directory username/password, pkcs12 (certificate/private-key) and its protection password, key material, pasteboard encryption key, SAML token, STA ticket, and Citrix PIN history.

The XenMobile server flag “ENCRYPT_SECRETS_USING_PASSCODE” controls whether Secret Vault should require user entropy to access. Based on server setting, Secure Hub will prompt users to set up a PIN code during enrollment. The PIN code is used as user entropy to derive a Secret Vault encryption key. If a PIN is not setup and the “ENCRYPT_SECRETS_USING_PASSCODE” flag is on, the Active Directory password will be used as user entropy to derive the key.
Kill Pill

Certain security features such as remote lock and wipe rely on the device receiving instructions from a server. If a device is lost or stolen and put into airplane mode before such an instruction is received, this could prevent corporate data from being destroyed. XenMobile MDX protects against this situation with a device-side “Kill Pill” feature which causes the container to lock or erase itself if it hasn’t been able to successfully connect to XenMobile Server within a configurable interval.
How is my data protected in transit?

MicroVPN

MicroVPN capabilities are a core feature of the MDX framework, granting secure access to enterprise resources for a number of functions including:

- Application access
- Intranet access
- Mail access (Negating the need for ActiveSync to be exposed directly on the firewall perimeter)

MicroVPN tunnels are unique per application, and encrypted to be protected from other device communication or other MicroVPN communication. In addition to security features, MicroVPN offers data optimization techniques including compression algorithms to ensure that only minimal data is transferred, and that the transfer is completed in the quickest time possible, improving user experience—a key success factor in mobile project success.

The following diagram outlines a typical network call established as part of the MDX policy definition within the XenMobile Server. Although the XenMobile Server defines usage of a MicroVPN, the NetScaler® will ultimately determine the path the client takes once it hits the gateway. (Note that XenMobile supports defining unique MicroVPN endpoints per application if required.)

Encryption Level for TLS Session

The encryption level for a TLS session can be defined on the Netscaler, but is typically AES-256.
How Is My Data Protected Inside the Company?

Security inside the company network is just as critical, if not more so, than the security on the mobile device. Citrix takes a number of measures to protect mobile management infrastructure. The primary components of a XenMobile solution include NetScaler and XMS. Standard security penetration testing is done to ensure that no exposed attack vectors exist.

NetScaler also provides a secure, scalable application firewall. The NetScaler firewall serves as the primary edge NetScaler Gateway/egress point. A vast number of security checks are performed at this point. For example, all logon input fields are protected against standard security threats.

XenMobile Server leverages a hardened Tomcat web services deployment customized for MDM and MAM.

Database services are enabled through Microsoft SQL Server (or Postgres for evaluation/testing purposes only). XenMobile Server is logically separated from the database. The database can reside anywhere, but best practice is to install the database inside the company network. **Thus, critical data, regardless of its state, will not reside in the DMZ.**

Authentication of users is provided by LDAP services in real time. This reduces the amount of data that must be stored in XenMobile Server and reduces potential exposure.

**Internal Controls**

Citrix adheres to secure development methodologies and processes internally, which include release gates and security activities such as design reviews, threat modeling, secure code review and application penetration testing.

**NetScaler**

The NetScaler and firewall configuration files for a device are located on protected disk storage within the physical or virtual NetScaler appliance. All administrative access to the device is controlled via authentication using a AAA subsystem, which supports locally defined users, users in Active Directory, other LDAP directories, or TACACS+.

**XenMobile Server**

Configurations are stored in the database, either onsite or on an external SQL server. Access is protected via authentication.

**XenMobile Apps**

All configurations are stored within the XenMobile Secure app using encryption. Users are able to edit certain parameters, but only upon authentication.
Citrix Receiver

Citrix Receiver stores only the fully qualified domain name of the Citrix Store to which it needs to communicate.

Cryptography

XenMobile utilizes an OpenSSL cryptographic library to protect data at rest on mobile devices and servers, as well as data in motion between these components. On iOS platforms, XenMobile also leverages strong platform-specific FIPS-validated cryptographic services and libraries such as keychain. OpenSSL is also well known for providing FIPS-validated modules for a variety of platforms. This further secures data in motion as well as certificates needed to manage and enroll devices.

Critical data needed to run at the device and server level is encrypted using AES-256 encryption. An example would be a service account configured in the system for access to critical resources. Passwords for these accounts must be saved in a secure manner. All such data is secured in files and databases using AES-256 format.

Device/Server Verification

XenMobile employs strong two-factor authentication to prevent possible attacks. Multiple levels of digital certificates form the foundation of the XenMobile security infrastructure. A device certificate is issued during the enrollment process and is required for communications between the device and XenMobile Servers. Citrix also supports user identification certificates in addition to device certificates.

The iOS enrollment-initiated installation of the Citrix enrollment client is signed and approved by Apple for the App Store.

Jailbreak status is validated prior to enrollment. On iOS, enrollment starts with a device certificate request using Simple Certificate Enrollment Protocol (SCEP) via the built-in MDM capabilities embedded in the iOS operating system. Device certificates are signed and issued by an embedded XenMobile Certificate Authority (CA). These certificates are used during communication to ensure that the device is what it says it is. From this point forward, basic device management is performed by authenticating the client with the appropriate client certificate based handshakes. Client certificates are generated by a 3rd-party trusted CA, such as when customers already have a PKI deployment in place. XenMobile supports most popular commercial CA services, such as Microsoft, Symantec, RSA, and OpenTrustCA.

Android enrollment is initiated via the Citrix enrollment client published on Google Play and Amazon Appstore. Basic user authentication is performed as explained above. The device is evaluated for rooted status and then authenticated. Once completed, certificates are exchanged. These certificates are passed from this point forward to authenticate the client for the XMS solution.

All data and certificates/private keys locally stored on the device are encrypted using AES-256 encryption in Citrix Secret Vault or a strong platform-native service such as iOS keychain.
Operational Security Features

XenMobile offers a full set of features to assist with day-to-day or operational security management of mobile devices, applications, and data. Operations teams get the control they need to enroll users, manage and wipe devices (or selectively wipe corporate apps and data), and to automate actions such as notifications and device compliance flagging. They can also maintain app and data integrity through advanced auditing capabilities, and ensure the protection of sensitive corporate assets with multi-layered DDoS protection.

Enrollment

There are basic differences between iOS and other managed platforms for enrollment with regard to the process of joining a device to the managed service. These are mostly due to the documentation and API’s offered by the device manufacturer.

There are a number of optional enrollment controls within XenMobile MDM that provide a balance between security and usability. These include a username (locally created or in Active Directory) in addition to one or more of the following 2nd factors:

<table>
<thead>
<tr>
<th>Factor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Password</td>
<td>Residing in AD or locally entered on server</td>
</tr>
<tr>
<td>A Server Generated PIN</td>
<td>It can be (x) characters, numeric or alpha</td>
</tr>
<tr>
<td>An Enrollment URL</td>
<td>Random unique URL that must be used on XMS</td>
</tr>
<tr>
<td>Derived Credentials</td>
<td>The credentials, derived from a smart card, reside on a mobile device instead of on the card</td>
</tr>
</tbody>
</table>

Additionally, each device enrollment may have the following attributes associated with it:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validity Time</td>
<td>How long the enrollment invitation is valid</td>
</tr>
<tr>
<td>Device Binding</td>
<td>To which device Serial/IMEI/UDID is this invitation bound</td>
</tr>
</tbody>
</table>

Alternatively, a SAML token may be used as a credential to pass validity from a SAML server such as Active Directory Federated Services (ADFS).
Initial Enrollment Flow Diagrams
The following sections describe initial enrollment using iOS as an example. Android enrollment is very similar.

MDM Enrollment
Enrollment is usually end-user driven, as part of either a reactive download from a device platform app store, or as part of notification generation at the server side.

After downloading the iOS Secure Hub Application, the user is prompted to enter a username or email address that will be used to authenticate within the service.

The domain portion of the entered email address is compared with the XenMobile Auto Discovery Service (ADS) to determine whether auto-population of the server address, port and additional security parameters is possible. If not, the user will be prompted to enter a valid server address.

The XenMobile Auto Discovery Service also facilitates Certificate Pinning, which provides Secure Hub with a certificate it can then compare with the certificate provided to it by XenMobile Server. If the certificate provided by XenMobile Server doesn’t match the certificate provided by ADS, then enrollment is not allowed to proceed.
The XenMobile Server enrollment service is checked for availability, and the user is authenticated against XenMobile Server, which also confirms that the device has not been revoked previously. XenMobile Server will use either local (database) or Active Directory authentication to confirm that the user is valid. At this point the user will need to have supplied a password and/or PIN depending on the enrollment type defined at the server.

After successful authentication, optional terms and conditions are presented. If a user fails to comply, they are not allowed to continue enrollment.

If the server has self-signed the root certificate, the user will then be prompted to accept a root setup of the enrollment of the device. An alternative would be to install a trusted certificate on XenMobile Server. At enrollment, a certificate is generated and installed on the client, which will represent the user for future MDM sessions. Once SCEP is complete, XenMobile Server instructs the APNS to notify the device to use this certificate to connect in to the standard XenMobile connection port to complete the enrollment, run the initial MDM session, collect inventory, etc.

Post Enrollment (Day-to-Day Connectivity)

Day-to-day management takes place in one of the four scenarios below:
- Scheduled deployment – where a deployment task is delayed until a specific time
- Scheduled inbound check-in – by default every 6 hours for iOS, also, configurable
- Ad hoc task – such as right-click lock/wipe/locate, activated by a console administrator
- Web service call
All events are triggered via an Apple Push Notification instructing the device to connect inbound over port 443. Apple Push Notification Service (APNS) is an Apple-specific notification method and service for secure notification of both “connect” events for MDM as well as general device notifications (e.g. message popups). APNS ensures only valid messages get pushed to devices, and that all MDM activity is associated with a server-installed certificate that is co-signed by the MDM provider.

For a further detailed description of APNS and its capabilities, Apple provides more information on their website:

When a device connects inbound to XenMobile Server, it presents a valid certificate containing the user ID of the device. This ID is used by the Active Directory “Bind User” function to check three attributes:

• Active Directory Group Membership
• User account is not disabled
• Active Directory attributes of the user (e.g. email address)

Optional security measures include the support of secure LDAP, where a certificate is used as additional authentication to support the lookup process of the Active Directory bind user.

MAM Enrollment
For customers that are running MAM-only or a combination of MDM and MAM, Secure Hub will interact with NetScaler Gateway and XenMobile Server to complete user authentication and registration. AMDX master encryption key and a MAM authorization token are generated during the enrollment.

Optionally, user certificates can be distributed at the end of enrollment, which improves user experience by eliminating the need for user password input after enrollment. In addition, Citrix PIN can be set up to allow users to use a PIN code instead of a password.

Remote Data Wipe
The safety net for data loss prevention is the ability to initiate removal of data from a remote device.

Wipe functionality is available at multiple levels including:

• Selective (corporate wipe)
• Full wipe (device reset)
• Container wipe

And can be initiated in the following ways:

• Administrator initiated (subject to role approval within console)
• User initiated (as part of the self-help functionality)
• Automated (as part of automated-actions, described below)
• Automated based on device inability to contact the server (Kill Pill)
• As part of some other process initiated via web service
**Application Execution Prevention**

On supported platforms, XenMobile can whitelist or blacklist applications and processes. This prevents both installation and execution of unauthorized tasks. Typical use cases include preventing access to public application stores, restricting leisure applications, or simply preventing configuration changes. This is achieved with a task watcher embedded within Secure Hub that is able to prevent interaction with any unauthorized execution.

**Web Services**

Because today's enterprises demand integration points, XenMobile offers a wide variety of REST based web interfaces, enabling simple automation and interaction with services such as user creation, admin tasks, and retrieval of asset and inventory information. These calls are secured via SSL to XenMobile Server. This approach has been a key differentiator when working with service providers to offer services such as billing integration and access from a unified portal.

**Automated Actions**

XenMobile provides automated actions that protect and inform both users and the security administrator in the event of an issue. An automated action can be used as an engine to perform a task or tasks should the device or user state change.

A typical example:

*IF User no longer employed with company (disabled in AD), THEN selective wipe of the device.*

This automates the un-enrollment process and drives security based on existing best practices. This process should remove user access to company systems, and also remove company apps, follow me data (cloud storage), cloud systems (SFDC, etc.) along with SSO credentials, etc.

These actions may be combined and can result in notifications, blocking, flagging as out of compliance, or wiping. The enterprise has the flexibility to make this choice. With the typical needs understood, let's examine how to secure enrollment and MDM components.

**Auditing Capability**

XenMobile leverages industry-recognized controls for maintaining SIEM data. In addition to audit trails for server-based activity, key user information can be gathered from gateway components, including time of access, IP address and device data.

**NetScaler**

Rich audit trails are recorded both on the appliance and streamed to configured external log collection servers.

**XenMobile Server**

Audit trails are stored in the central XenMobile Server database, and XenMobile Server provides out-of-the-box audit trail reports, which include user info, activity info, date/time stamps, etc., for administrative actions and more. XenMobile Server does not (by default) expire audit trails and
information from the database. XenMobile Server also provides different levels of server logging and verbose logging if needed during troubleshooting exercises. No data is shown in log files; however, log files will contain user information such as logon user ID, with password information excluded. Many device policy violations—such as jailbreak, unmanaged device, location perimeter violation, or location disabling—can be configured to generate automatic alerts. Application, device, and user login events are all recorded in audit logs. Different levels of log and audit info, warnings, and errors can all be configured on a per-module basis. This information is available for access by sending log files to a system log (syslog) server.

**Ensuring Denial of Service Protection**

**NetScaler**

All logon input fields are protected against standard security threats. DDoS protections defend against malicious clients.

**XenMobile Server**

Security penetration testing is done to identify and remediate attack vectors. Additional app firewalling is possible via NetScaler.

**Citrix Receiver**

Our common SDL practices dictate the use of various means to detect buffer overruns during development phases, including run time tools, fuzzing libraries, etc.

**XenMobile Apps**

For XenMobile Apps we do not perform any explicit input or sanity checking on the incoming data from NetScaler or other enterprise resources, such as Microsoft Exchange. We trust that the server is sending us a valid stream.

**PKI Integration and Distribution**

XenMobile Server can make certificate requests to external certificate service providers such as Microsoft, Entrust, Intercede, or RSA via web enrollment to enable certificate-based authentication for WIFI, VPN and Exchange ActiveSync profiles. The end game is to provide controlled, authenticated access to network resources— but only for devices that are compliant with company security and compliance requirements. Certificates can provide access to network resources without the need for user interaction, or serve as a second authentication factor.

This can be done by acting as a client and requesting certificates on behalf of users with enrolled devices or configuring the device to communicate directly with the CA using Simple Certificate Enrollment Protocol (SCEP).

Certificate revocation and renewal are also supported, driving a balance between security and usability.
Summary

EMM/UEM is the key to managing personal devices in a corporate setting at scale – without impacting user experience, and without inflating costs or introducing security risks.

Citrix XenMobile delivers the powerful end-to-end EMM solution you need. By combining the essential features of MDM and MAM, XenMobile gives you complete control over mobile apps and data, centralizes mobile device and user management, and shields your network from mobile threats.

The XenMobile solution – with integrated Citrix products – enhances employee productivity and enables secure remote access to applications. Citrix Secure Hub provides a comprehensive set of mobile productivity apps, while Citrix NetScaler Gateway fortifies the network and lets IT control how users access their applications and data.

XenMobile uses a broad range of technologies and standards - including authentication, encryption, containers, policies, passwords, certificates, and micro VPNs – to provide enterprise-class security and compliance in key mobility use cases, allowing you to protect data:

- At rest
- In transit
- Within the company

In addition, XenMobile lets you manage ongoing operational scenarios including user and device enrollment, remote data wipe, and auditing.

Only Citrix delivers a single integrated EMM solution to manage mobile devices, mobile apps, desktops, and desktop applications. This integrated approach helps IT further reduce costs by leveraging the same architecture, hardware and devices for end-to-end application and data delivery. XenMobile facilitates positive user experiences that improve productivity and help eliminate shadow IT while ensuring employee privacy and providing enterprise-grade protection for the corporate data and assets that matter most.
References and appendices

XenMobile MDX-Enabled Applications

An enterprise can obtain MDX-enabled applications in one of three ways:

• Wrap existing mobile applications using XenMobile Application Wrapping.
• Build your own application and including the MDX SDK (single line of code).
• Download a partner-enabled application from the Citrix Ready Marketplace.

Each Citrix MDX-enabled application will have an extensive policy library (over 60 policies) but also includes app-level encryption.

Using the Citrix MDX SDK, IT can:

• Separate business and personal apps and data in a secure mobile container where they can be secured with encryption and other mobile DLP technologies and can be remotely locked and wiped by IT.
• Enable seamless integration between Citrix MDX-enabled apps while also controlling all communication so IT can enforce policies, such as ensuring that data only is accessible by Citrix MDX-enabled apps.
• Provide granular, policy-based controls and management over all HTML5 and native mobile apps, including an application-specific micro VPN for accessing an organization’s internal network, preventing the need for a device-wide VPN that can compromise security.

The following appendix sections lists the MDX app policies for iOS, Android, and Windows Phone and for the XenMobile Apps.

Logical Component Diagram
About the Authors and Contributors

Frank Srp is a Senior Technical Marketing Manager specialized on Mobility, Citrix.
Matthew Brooks is a Senior Technical Product Marketing Manager specialized on Mobility, Citrix.
Mike Bowlin is a Senior XenMobile Architect, Citrix

A special thanks to the reviewers of this XenMobile Security Whitepaper:
• Mike Hogan
• Kevin Binder
• Amandeep Nagra
• Tarkan Kocoglu