XenMobile Security

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

CITRIX®

Contents

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. 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 only becomes active when a particular application is accessed. This, in turn, has evolved to encompass app-level control of secured "micro-VPNs," inter-container communication, and encrypted sandbox containers.

More recently, **Enterprise Mobility Management (EMM)** suites have emerged, 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.

Of course, an EMM 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.
- WiFi networks.
- Application management/push technology.
- Monitoring products.
- IDS.
- Workflow Automation.
- System imaging technology.
- Policy management.

An EMM 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.

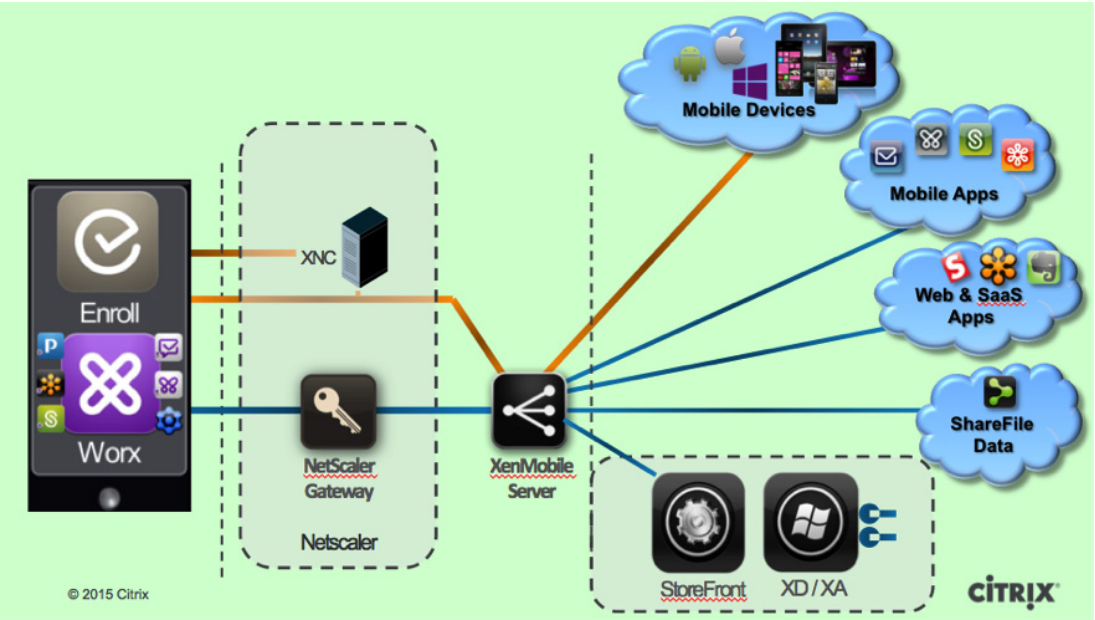
Citrix mobility solution - XenMobile

Citrix® XenMobile® provides comprehensive, end-to-end security, and delivers the full breadth of EMM capabilities without sacrificing an engaging user experience.

In fact, only Citrix delivers a single integrated EMM solution to manage mobile devices as well as 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 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.

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 sever offers a single console for management of devices, apps, and data.

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.

XenMobile MDM provides:

- Device-level password protection.
- Encryption.
- WiFi.
- Device inventory.
- Application inventory.
- Selective/full device wipe.
- Specific device manufacturer APIs (Samsung, HTC, etc.)
- Automated Configuration of WiFi.
- Restricted access to device resources: App Stores, camera, browser, etc.

You can use XenMobile MDM to manage iOS, Android, Windows 8, Windows Phone 8+, Windows Mobile, and Symbian mobile devices.

From the XenMobile web console, you can:

- Import users from your Active Directory user database.
- Enroll users and their devices with multi-factor security:
- Create and deploy policies.
- Define and enforce compliance standards.
- View reports.
- Set application blacklist and whitelists.
- Configure an email server.
- Locate devices.
- Remotely wipe lost or stolen devices.
- Configure advanced PKI certificates or SAML authentication.

In addition, the XenMobile Server allows you to:

- Onboard mobile devices.
- Automatically deploy device management configuration on the mobile device that includes:
  - Policies (security policies, restrictions, device configurations and settings, etc.)
  - Software packages / App Delivery
  - Registry keys / XML configuration files
  - Files
  - Scripts
- Deploy packages for devices, users, and groups, with the ability to restrict deployment based on comprehensive rules and scheduling.
- Have visibility and auditing including: user and device management configurations and settings, device hardware, software inventory, and connection logs.
- Enable high availability and scalability through a multi-server redundant architecture and load balancing to support very large deployments.
- Remotely control, lock/unlock, wipe, etc.
- Take advantage of roles-based administration and delegation.
- Obtain online mobile activity reports, providing detailed information on users, devices, policies, and deployment packages.

XenMobile Mobile Application Management (MAM)

XenMobile provides the 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. Users access their applications through Citrix Receiver™ or Receiver for Web sites.

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.
- 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:

- AES-256 encryption is provided for files and DBs on mobile devices. 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 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 application specific polices 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, Android, and Windows Phone systems.

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 Worx Gallery – 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 architecture

Worx Home

Worx Home is the central control point for all XenMobile wrapped or compiled applications as well as content stored on the device. WorxHome 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 Worx Home 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.

XenMobile Security Details

Application Authentication Controls

Worx Home serves as the encryption key broker for all MDX applications. Each application under management retrieves its policy check-in times from the WorxHome 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 Worx Home application connects to the XenMobile server(s) a unique token is generated by Worx Home and passed to the XenMobile services running on the XenMobile server appliance.

XenMobile server provides Citrix specific application management and policy control for MDX based applications. The XenMobile Server validates this user/device from an asynchronous connection to the NetScaler to ensure the device is who it claims to be and that the NetScaler has successfully authenticated it.

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

Worx Home 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. WorxHome 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.

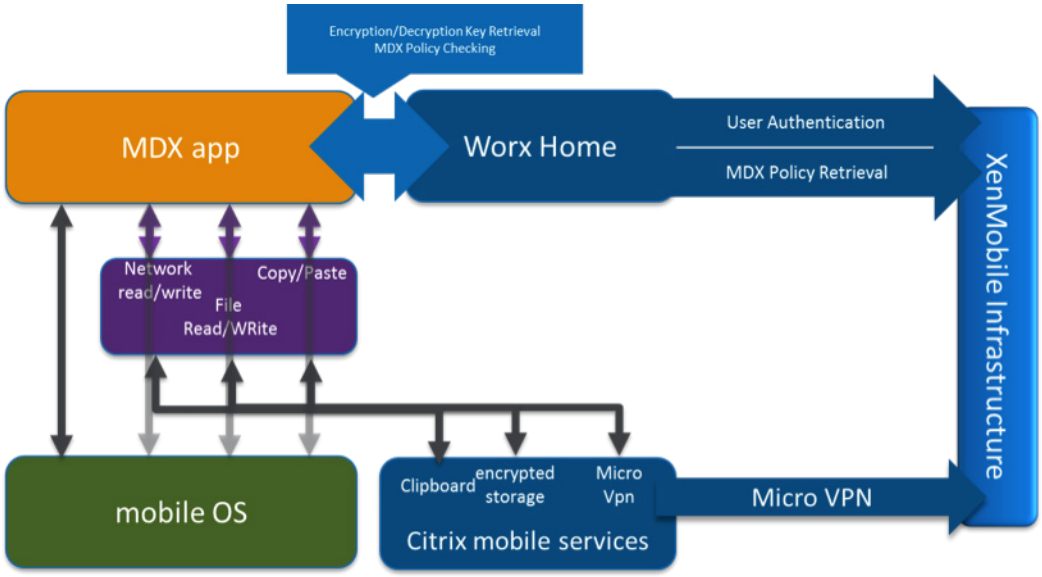
Worx Home utilises these cryptographically strong variables to generate an AES encryption key. The encryption key on iOS and Android are both AES-256 bit keys.

The resultant key is then used by the MDX applications to encrypt all of its data prior to writing it to the device. The same key is the used to receive/decrypt all data at rest.

FIPS 140-2 Compliance

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

Platform	Location	Strength	Key Location
IOS	MDX Applications	AES-256	Citrix Secret Vault
Android	MDX Applications	AES-256	Citrix Secret Vault
WindowsPhone	MDX Applications	AES-256	

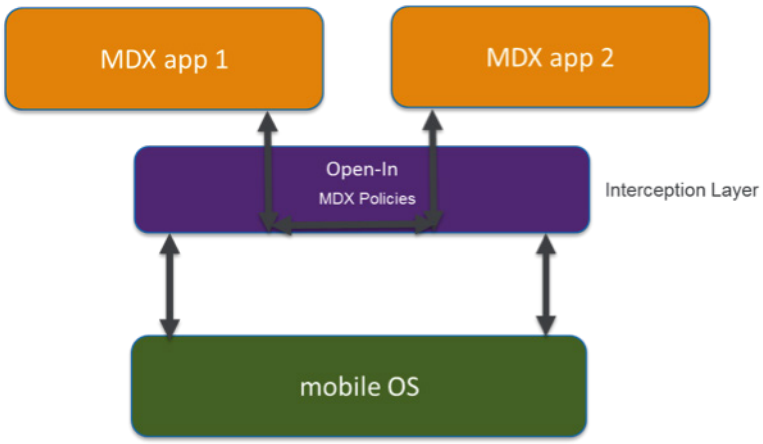
How is my data protected at rest?

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.
- 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.).

This has been outlined below in a functional diagram:



This table provides a summary of encryption key location and strength by mobile platform:

Platform	Location	Strength	Key Location
IOS	MDX Applications	AES-256	Citrix Secret Vault
Android	MDX Applications	AES-256	Citrix Secret Vault
WindowsPhone	MDX Applications	AES-256	

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 Worx Home and other Worx 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 with a split key where the key encryption key is stored on the device, and a more secure form where the key encryption key is composed of user entropy that must be entered by the user of 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 worxPIN history.

The XenMobile server flag "ENCRYPT_SECRETS_USING_PASSCODE" controls whether Secret Vault should require user entropy to access. Based on server setting, WorxPIN will prompt users to set up a PIN code during enrollment. The Worx PIN code is used as user entropy to derive a Secret Vault encryption key. If Worx 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.

How is my data protected in transit?

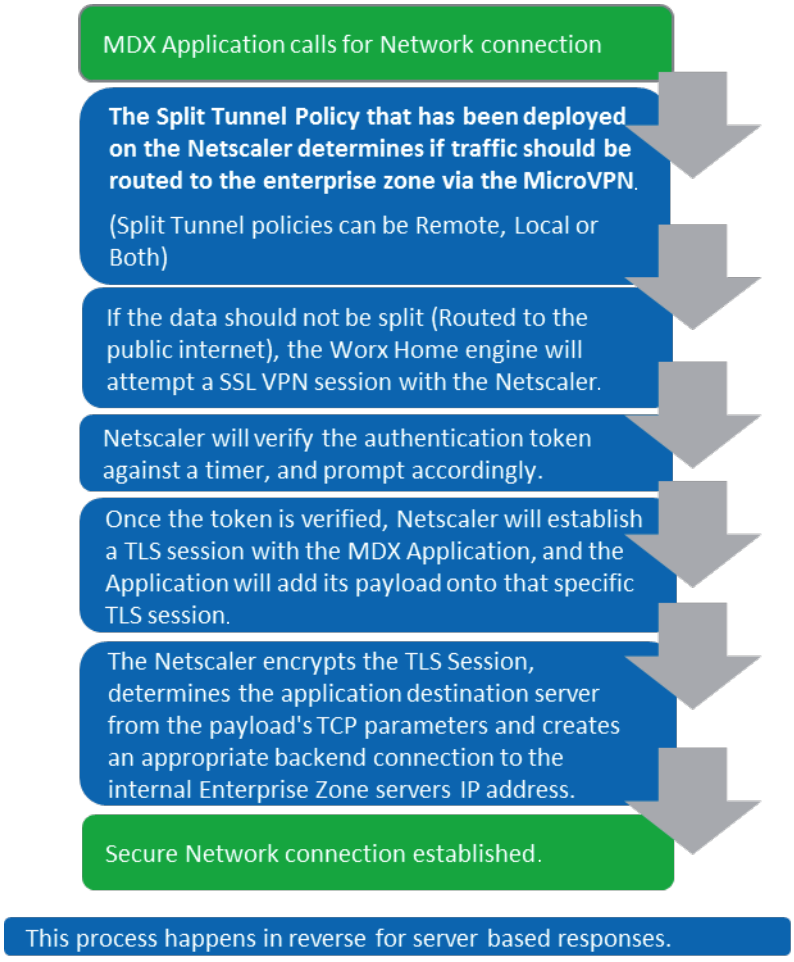
MicroVPN

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's offer 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.



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.

The XenMobile server leverages a hardened Tomcat web services deployment customized for MDM and MAM management.

Database services are enabled through Microsoft SQL Server or Postgres (for evaluation/testing only). The 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 the XenMobile server system and reduces potential exposure.

Internal controls

Citrix has an independent security team that is not part of the XenMobile product group. This group performs penetration testing, evaluates the product software much like an external entity would, and flags security concerns, which are prioritized across levels of critical, high, medium and low severity. Citrix engineering teams are expected to respond back to the concerns with fix schedules before the product is certified as ready for release.

Citrix also subjects the XenMobile product to external penetration tests by reputable external security vendors. Verification letters and penetration reports are available.

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 and 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.

Worx mobile apps

All configurations are stored within the Worx app using encryption. Users have a UI to edit certain parameters, which is accessible only upon authentication.

Citrix Receiver

Citrix Receiver stores only the configuration of the Citrix Store fully qualified domain name 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 Worx 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 either an embedded XenMobile Certificate Authority (CA) or 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 OpenTrust 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.

Android enrollment is initiated via the Worx 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 remotely, and to automate actions such as notifications and device 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:

Factor	Description
A Password	Residing in AD or locally entered on server
A Server Generated PIN	It can be (x) characters, numeric or alpha
A Enrollment URL	Random unique URL that must be used on XMS

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

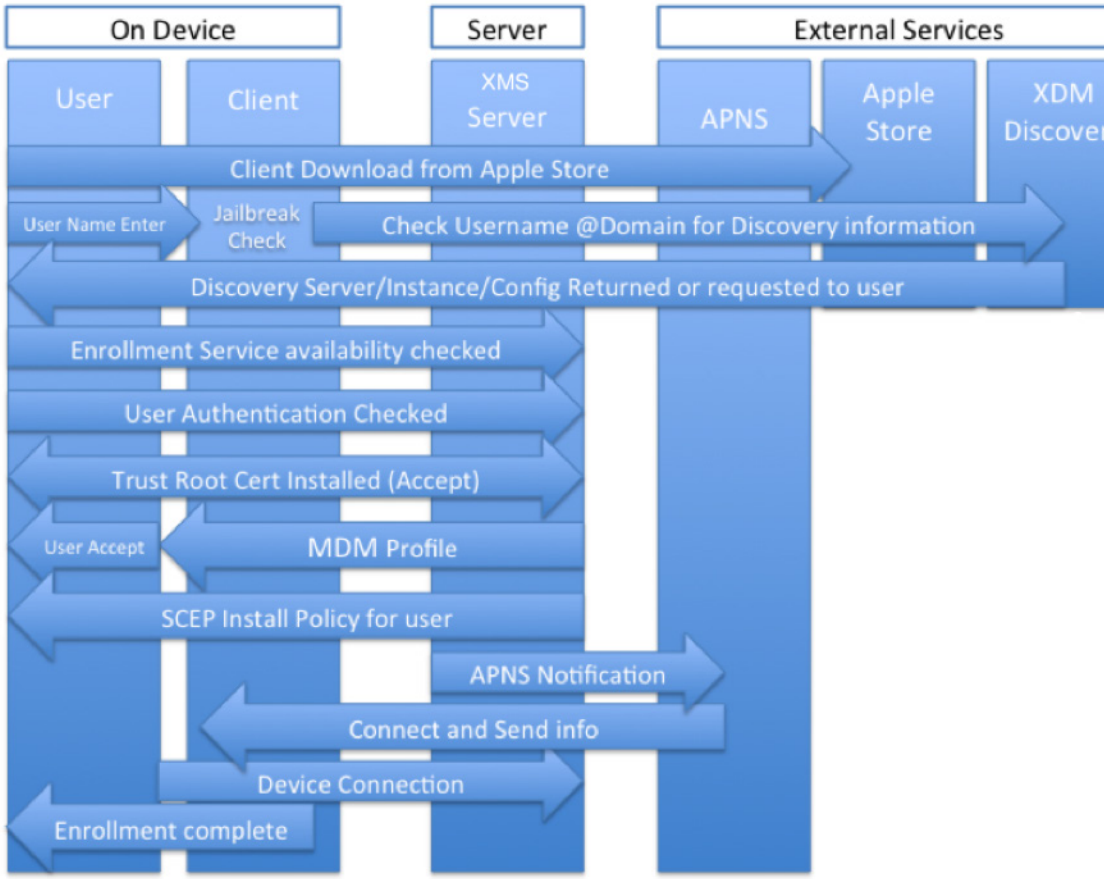
Attribute	Description
Validity Time	How long the enrollment invitation is valid for
Device Binding	Which device Serial/IMEI/UDID is this invitation bound to

Alternatively, a SAML token may be used as a credential to pass validity from a SAML server such as Active Directory Federated Services (ADFS).

iOS initial enrollment flow diagrams

MDM enrollment

Enrollment is usually end-user driven, as part of either a reactive download from the iTunes store, or as part of notification generation at the server side:



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

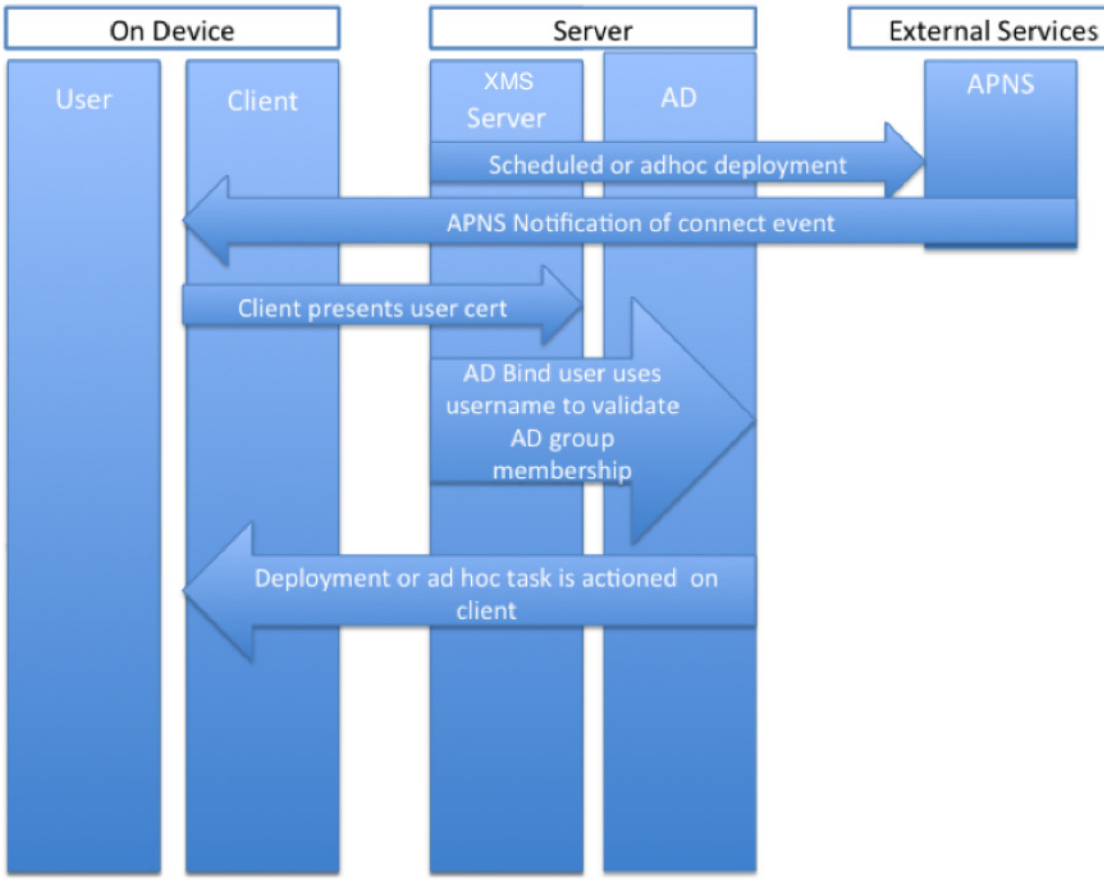
The domain portion of the entered email address is used against the XenMobile discovery service to validate if auto-population of the server address, port and additional security parameters are available. If not, the user will be prompted to enter a valid server address.

The XenMobile server Enrollment service is checked for availability, and the user is authenticated against the XenMobile server, which also confirms that the device has not been revoked previously. The 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 set up of the enrollment of the device. An alternative would be to install a trusted certificate on the 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, the 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.
- Adhoc 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:

http://developer.apple.com/library/mac/#documentation/NetworkingInternet/Conceptual/RemoteNotificationsPG/Chapters/ApplePushService.html#//apple_ref/doc/uid/TP40008194-CH100-SW9

When a device connects inbound to the XenMobile server service, 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 only running MAM or a combination of MDM and MAM, WorxHome will interact with NetScaler Gateway and the XenMobile server AppC service to complete user authentication and registration. An MDX 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, Worx 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).
- 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 in the client 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 the XenMobile server. This approach has been a key differentiator when working with service provider partners to offer billing integration and access from a unified portal.

Automated actions

Every solution should provide 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/full wipe of the device.

This automates the un-enrollment process and drives security based on existing best practices. This process should remove the user from 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, lets 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 Citrix 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 (which is mainly user 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 via Simple Network Management Protocol (SNMP).

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.

Worx mobile apps
For Worx 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, or RSA via web enrolment to enable certificate-based authentication for WIFI, VPN and Exchange ActiveSync profiles. The end game is to provide controlled, authenticated network resource access to devices – but only for devices that are compliant with company

security and compliance needs. Certificates can provide access to network resources without the need for user interaction, or serve as a second level of authentication.

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 catered for driving a balance between security and usability.

Summary

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.

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 Worx Home 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 Worx MDX-enabled applications

An Enterprise can obtain Worx-enabled applications in one of three ways:

- Wrap existing mobile applications using XenMobile Application Wrapping.
- Build your own application with the Worx SDK.
- Download a partner-enabled application from the Worx gallery.

Each Worx-enabled application will have a common set of policies and capabilities, listed below:

Application Specific Policy	
Cut and copy	Blocks, permits or restricts clipboard cut/copy operations for this application. When set to "Restricted," the copied clipboard data is placed in a private clipboard that is only available to MDX applications.
Paste	Blocks, permits or restricts clipboard paste operations for this application. When set to "Restricted," the pasted clipboard data is sourced from a private clipboard that is only available to MDX applications.
Document exchange (open-in)	Blocks, permits or restricts document exchange operations for this application. When set to "Restricted," documents may only be exchanged with other MDX applications.s.
App URL schemes	iOS applications can dispatch URL requests to other applications that have been registered to handle specific schemes (such as "http://"), providing a mechanism that enables one application to pass requests for help to another. This policy serves to filter the schemes that are actually passed to the application for handling (i.e. inbound URLs).
Allowed URLs	This policy serves to filter the URLs that are passed from this application to other applications for handling (i.e. outbound URLs).

Specific restrictions at a Worx-enabled application level:

Application Restrictions	
Location services	When set to "On," this policy prevents an application from utilizing location services components (GPS or network).
AirPrint	When set to "On," this policy prevents an application from printing data to AirPrint-enabled printers.
Camera	When set to "On," this policy prevents an application from directly utilizing the camera hardware on the device.
SMS compose	When set to "On," this policy prevents an application from utilizing the SMS composer feature used to send SMS/text messages from the application.
Email compose	When set to "On," this policy prevents an application from utilizing the email compose feature used to send email messages from the application.
iCloud	When set to "On," this policy prevents an application from utilizing Apple® iCloud features for cloud-based backup of application settings and data.
Microphone recording	When set to "On," this policy prevents an application from directly utilizing the microphone hardware on the device.

Authentication settings at a Worx-enabled application level:

Authentication settings	
Re-authentication period (hours)	Defines the period before a user is challenged to authenticate again. If set to zero, the user is prompted for authentication each time the app is started or activated.
Maximum offline period (hours)	Defines the maximum period an application can run offline without requiring a network logon for the purpose of reconfirming entitlement and refreshing policies.
Offline access permitted after challenge	The app prompts the user to log on but allows offline usage after PIN/passcode/password challenge.
Offline challenge only	The app challenges the user for an offline PIN/passcode/password.
Not required	The app does not require the user to log on.

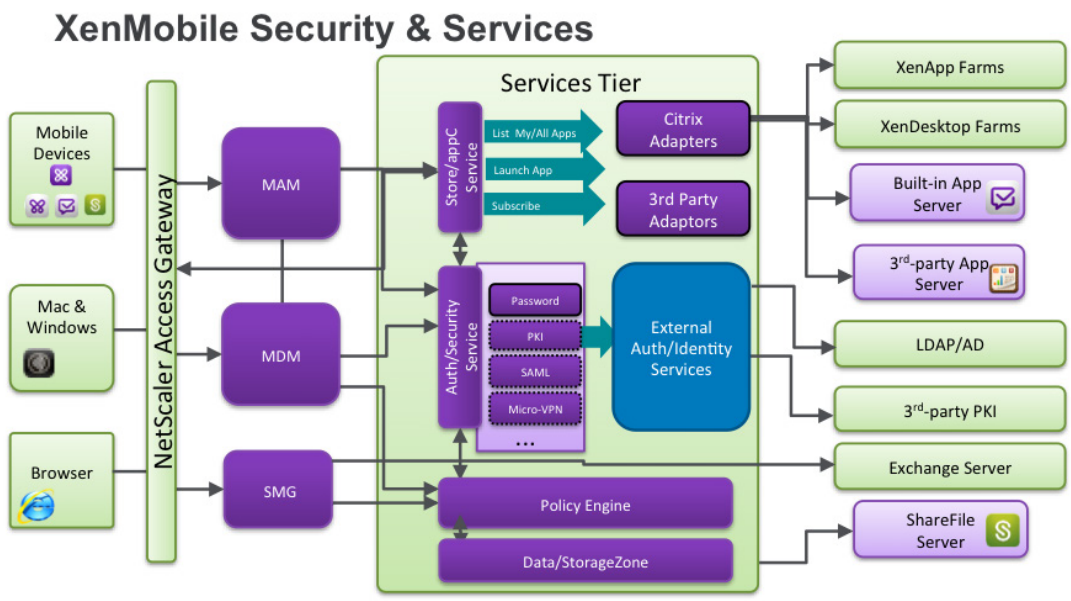
Security settings at an enabled Worx application level:

Security Settings	
Black, jailbroken and rooted devices	When set to "On," the application is locked when the device is jailbroken or rooted. If set to "Off," the application can run even if the device is jailbroken or rooted.
Enable database encryption	When set to "On," this policy ensures that the data held in local database files is encrypted. When set to "Off," the data held in local databases is not encrypted.
Encryption keys	When "Online access only" is selected, secrets used to derive encryption keys may not persist on the device. Instead, they must be recovered from the CloudGateway key management services each time they are needed. When "Offline access permitted" is selected, secrets used to derive encryption keys may persist on the device. When set to "Online access only," the authentication policy is assumed to be "Network logon required" regardless of the authentication policy setting that is actually configured for the app. When set to "Offline access permitted," it is recommended (but not required) that the authentication policy be set to enable an offline password challenge, which will protect access to the keys and associated encrypted content.
Erase app data on lock	When set to "On," and an application is locked, any persistent data maintained by the app is erased, effectively resetting it to its just-installed state. If off, application data is not erased when the app is locked. An application can be locked for any of the following reasons: loss of app entitlement for the user, app subscription removed, Citrix Receiver account removed, Citrix Receiver uninstalled, too many app authentication failures, jailbroken or rooted device detected without a policy permitting apps to run on jailbroken/rooted devices or device placed in lock state by administrative action.
Auth failure before lock	This sets the number of consecutive failed offline authentication attempts that will cause an app to become locked. Once locked, apps can only be unlocked through a successful enterprise logon.
App update grace period (hours)	Defines the grace period for which an app may be used after the system has discovered that an app update is available.
Active poll period (minutes)	When an application starts, the MDX framework polls CloudGateway in an attempt to determine current application and device status. Assuming CloudGateway is reachable, it will return information about the lock/erase status of the device and the enable/disable status of the application that the MDX framework will act upon. Whether CloudGateway is reachable or not, a subsequent poll will be scheduled based on this interval. After this period expires, a new poll will be attempted.

Network settings at an application level:

Network Settings	
Network access	Prevents, permits or redirects application network activity. If "Unrestricted" is selected, no restrictions are placed on network access. If "Blocked," all network access is blocked. If "Tunnelled to the internal network" is selected, a micro VPN tunnel back to the internal network is used for all network access.
Require internal network	When set to "On," the app is allowed to run only from inside the company network. The application will be blocked when the device is not connected to an internal network as determined by CloudGateway beacons. If "Off," the app can run from an external network.
Require Wifi	When set to "On," the app is locked when the device is not connected to a Wifi network. If set to "Off," the app can run using 4G/3G or LAN connections even if the device does not have an active Wifi connection.
Internal Wifi networks	Allows a comma separated list of allowed internal Wifi networks. From inside the company network, app access is blocked unless the device is associated with one of the listed network SSIDs. If this field is empty, any internal Wifi network may be used. If logged on from an external network (or not logged on), this policy is not enforced. The app requires a connection to one of the wireless networks specified.

Logical Component Diagram



CITRIX®

About Citrix
Citrix (NASDAQ:CTXS) is leading the transition to software-defining the workplace, uniting virtualization, mobility management, networking and SaaS solutions to enable new ways for businesses and people to work better. Citrix solutions power business mobility through secure, mobile workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. With annual revenue in 2014 of $3.14 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com.