XenMobile Security

Security is a top priority at Citrix. This whitepaper is meant to delve into the technical details of the security around the Citrix XenMobile solution and each of its components. Details include how Citrix implements secure mobile device management, mobile application management, mobile content management and more.

CITRIX®

Table of Contents

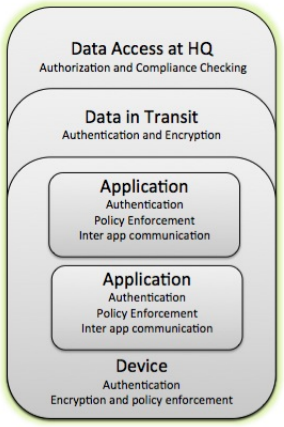
Foreword 3
Critical mobility requirements 5
Mobile device management with XenMobile 6
  Device operating system features 6
Jailbreak/rooted status 7
  Geo-location policies 7
Per-application encryption and policies 9
XenMobile architecture 9
  Component description 10
  NetScaler Gateway 11
  Device manager 12
  App controller 13
  Citrix productivity apps 15
    WorxMail 15
    WorxWeb 15
    Worx Home 15
XenMobile encryption and security 16
  How is my data protected at rest? 17
  How is my data protected in transit? 18
    Micro-VPN 18
  How is my data protected at HQ? 19
User enrollment 21
  Device enrollment 21
  APNS 22
  iOS initial enrollment flow 23
Additional security features 25
  IT automation 25
  Application execution prevention 26
  Web services 26
  Automated actions 26
  Auditing capabilities 26
  Denial of service protection 27
  PKI integration and distribution 28
References and appendices 28

An enterprise needs to take a holistic view to its mobility needs and ask the following questions:

- What are the immediate problems I need to solve?
- What are the issues I might need to solve in the future?
- Can I afford to take a 'piecemeal' approach to mobility or do I need a strategy that will solve my immediate and long term requirements as mobile adoption grows within the organization?

Mobility is a top priority for organizations. More employees than ever before are demanding access to the apps and data that will make them productive when they are outside the office, but this isn't as easy as it was in the past. Now, employees want this access from any mobile device, including their own personal devices. In addition, the apps that people need to get their jobs done have expanded beyond mobile email to include Windows, web and native mobile apps, both in the cloud and in the data center, and these apps are broadly distributed across different locations. However, for IT, allowing users to access all of their apps and data from untrusted devices raises significant security and network scalability concerns.

Depending upon their level of mobile adoption, enterprises have turned to either Mobile Device Management (MDM) solutions to manage the devices, and/or mobile application management (MAM) solutions to address data and app security. However, MDM and MAM solutions alone are not enough to ensure that scalable, optimized, high-performance apps are delivered to any user at any location. To be effective, these solutions also need the right network infrastructure in place to ensure that applications can be delivered across different devices securely, while addressing performance, manageability and future expansion considerations.



IT is accustomed to having full control of systems because they are provided by the company. When a BYOD model is employed, locking down features is generally no longer an option. And given the portability of these devices, further security controls need to be put in place to ensure data is protected.

Common tools include:

- Firewalls
- VPNs
- WiFi networks
- Application management/push technology
- Monitoring products
- IDS
- Workflow automation
- System imaging technology
- Policy management

The same methodology holds true for the Enterprise Mobility Management strategy in the mobile space. Today's mobile platforms and strategies require multiple layers of controls to ensure end users' needs are addressed while still ensuring that company data is protected.

XenMobile® leverages the vast scale and security expertise of the existing Citrix® products to create a more robust mobile solution.

From the beginning, **Mobile Device Management** has evolved from a 'niche component of the year 2000' through to a 'must have component of the year 2010' through to an expected underpinning foundation of any mobile strategy today. Its core focus lies around device level policy management, application delivery and data security.

Mobile application management was born more recently, focussing on securing and managing an application as an individual component, offering a quite similar set of policies and user experience management, but only active when the particular application is accessed. This in turn has evolved to contain app level control of secured 'MicroVPN's', inter-container communication and encrypted sandbox containers.

Mobility and the consumerization of IT pose key challenges for IT around scalability, security and application visibility. Citrix solutions including Citrix XenMobile provide a complete, integrated and scalable solution to deliver apps and data to any device with a secure and high performance user experience.

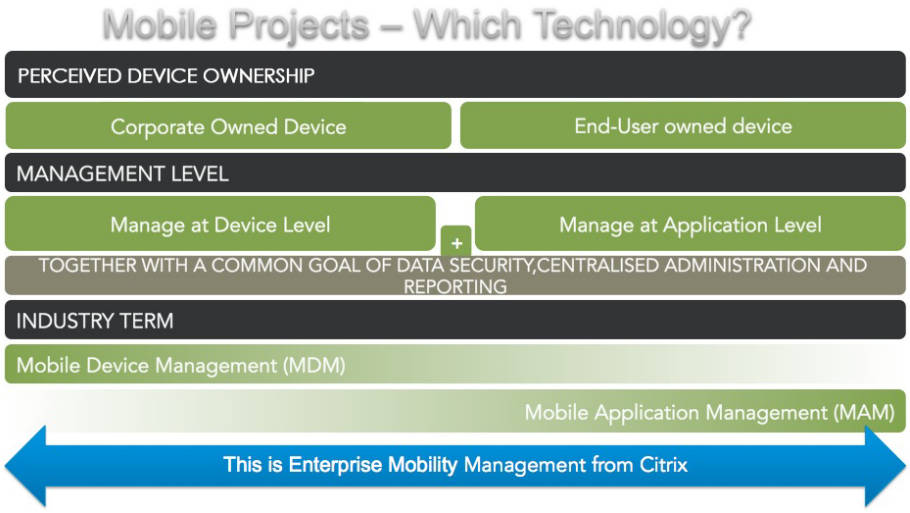
Besides application and device management, network and application delivery considerations need to be made for a full mobile solution. An integral part of any mobile solution should include an application delivery controller. XenMobile implements this technology via the Citrix NetScaler® product line. In the context of XenMobile, the NetScaler acts as a network policy enforcement point and SSL-VPN gateway, requiring users to authenticate at the perimeter.

NetScaler serves a critical role in scalable controlled access into the network. No other mobility solution in the industry includes the level of scale provided by NetScaler. NetScaler is used in some of the largest tech providers today, including Google and Apple.

A single NetScaler can scale to handle in excess of over 65,000 devices while still providing Denial of Service (DoS) attack protection, SSL off-loading, SSL application specific micro-VPN, user authentication and ActiveSync mail filtering. Compare this to the typical MDM vendor that struggles to handle this level of service at the 5-10,000 device range.

It is now clear that mobility strategy is touching key aspects of business initiatives in virtually all device management deployments. It is critical that companies select a vendor that can provide industry trusted perimeter access and scalability to meet the coming needs of any business initiative. As part of the XenMobile solution, devices/networks inherit the NetScaler protections given the integrated nature of the solution. Any mobility solution should include this component as an integral part of the network management.

These, coupled with the ability to control costs are the foundation of **Enterprise Mobility Management**.



An EMM solution requires an evaluation of the business needs, user needs and work – life considerations. Many organizations are using their mobility initiative to re-think the way they provide services to their end users. This includes SaaS, public/private clouds, application / desktop virtualization, application layer firewalls/NetScaler Gateways, SAML and certificate services to name a few.

Critical mobility requirements

IT needs a **complete stack of products** to address the needs of the business. Many users no longer consider their company IT resources to be ahead of the technology they have at home. This is driving user demands that IT must address. Users have easy, inexpensive access to productivity applications, cloud services and platform integration. IT must provide easy to use, secure tools to manage these devices or users will search for ways to work around security controls.

Critical mobility needs include:

- Device- or application-level password
- Device- or application-level encryption
- Geo-location services as an additional context
- Application delivery
- Selective/full device wipe
- Restriction enforcement
- OS level device configuration
- Secured/controlled cloud storage (follow me data)
- Application-level policy management
- Application-level secured access to the network
- Regulated environments: containerized email, etc.
- Secure browser

Mobile Device Management with XenMobile

MDM provides the foundation for configuring, managing and securing devices in any mobility strategy. This includes BYOD and devices provided to the end user. In the case of the Citrix EMM solution, XenMobile Device Manager provides this functionality.

XenMobile Device Manager ensures that the necessary OS hooks are in place to enforce/manage features including:

- Device-level password protection
- Encryption
- WiFi
- Device inventory
- Application inventory
- Full/selective wipe
- Specific device manufacturer APIs (Samsung, HTC, etc.)
- Automated configuration of WiFi
- Restricting access to device resources: app stores, camera, browser, etc.

Device operating system features

Mobile device operating systems continue to evolve and enhance security features on their respective operating systems. These enhancements have taken these devices from very insecure to out-of-the-box acceptable security for many of today's use cases for non-critical data. Any mobile solution should take advantage of these facilities and build upon them.

iOS and Android, for example, have built-in encryption for the device as a whole. Apple iOS has AES-256 encryption enabled as soon as a password is enabled on the device.

By providing this level of encryption, the National Institute of Standards and Technology (NIST), which examines and tests mobile devices for security and validation purposes, granted the Apple mobile platform FIPS 140-2 certification (Level 1).

This allows devices running the iOS 6+ operating system to be used in conjunction with the several Federal Government use cases.

Disk encryption on Android is based on dm-crypt, which is a kernel feature that works at the block device layer. The actual encryption used for the filesystem is 128 AES with CBC and ESSIV:SHA256. The master key is encrypted with 128 bit AES via calls to the openssl library.

XenMobile enables these features and tracks their status throughout the device life cycle. This data is also available to the Automated Actions engine. Automated actions allow the administrator to take proactive measures to protect the device when security is compromised in some way. Automated action is covered later in the paper.

Jailbreak/rooted status

One of the key components of this verification is determining the jailbreak/rooted status of the device. Virtually all device compromises are either achieved by root/jailbreak status or via OS security holes/bugs.

A few security white papers have been released that discuss security flaws in MAM. The most notable scare tactic used in these docs access to /proc/-ProcessID-/mem. By default a user does not have access to this file. The illustration of a standard device is listed below. Note that read/write access (rw) is only for the root user on the device. This access can only be accomplished via rooting/jailbreaking a device.

```
127|shell@android:/proc/31746 $
127|shell@android:/proc/31746 $
127|shell@android:/proc/31746 $ ls -al mem
-rw------- root     root              0 2013-06-10 13:09 mem
shell@android:/proc/31746 $
```

Hence, serious consideration should be placed on ensuring strong jailbreak/rooted status. As of this writing Citrix is the only player in the Gartner Magic Quadrant that detects jailbreak status prior to enrollment in the MDM solution.

Citrix XenMobile leverages a number of proprietary methods to detect jailbreak and root status. This includes API availability, binary inspection, installed applications and other means. This includes timers which control access and verification on admin specified intervals to verify jailbreak/root status.

Once device level protections are put in place, the security admin should now focus on ongoing controls to protect device data post enrollment/install. This includes device inventory of applications, available storage, status of the user in AD, etc.

Geo-location policies

Location services can be employed for a variety of use cases. The most common use case of location services is to find lost devices. Recovering a lost device with private information on it protects the company from falling out of compliance.

Privacy concerns in a number of countries is a legal concern as tracking a user typically must be agreed to by the end user. XenMobile offers controls to enable this feature globally, group or even user level. Further role-based access controls are available to control who can request the data as well as who can view the data.

Location services can be used to establish a geo-perimeter; this use case is common in hospitals that are protecting data on a nurse's station medical cart. Systems in this case should not leave the hospital. Administrators can establish a geo-perimeter. If the device leaves the perimeter all contents can be fully or selectively wiped.

Mobile application management with XenMobile

The MAM feature set of the Citrix solution, known as MDX, provides a single, secure storefront or interface for mobile devices to access both public and private apps. In addition, it provides a springboard to virtual apps and desktops from the mobile platform as well - your VDI and virtual application initiatives for desktops are fully portable as part of the Citrix mobile platform. Public stores include such products from Apple, Google and Amazon. Private app stores include apps developed in house for distribution to devices. These apps can leverage the Citrix compile time embedded policies or post compile via wrapping. In addition, there is a hybrid approach which includes public apps which have been specifically programmed to leverage XenMobile application wrapping policies. The Citrix app catalogue is 2x that of any other vendor as of this writing.

MDX builds on XenMobile Device Manager (XDM) by leveraging the SSL communication channel between the MDM client (Worx Home™) and the NetScaler Gateway™ which is typically deployed in the company DMZ. Building on this technology is the Citrix MDX technology, often generally referred to the market as MAM.

Built into the solution is a secure web browser, a mail/calendar/contact container and Citrix ShareFile®, a follow me data solution. This provides:

- Ability to seamlessly browse intranet sites without the need for expensive VPN solutions that open the company network to all applications on the device.
- AES-256 encryption for files and DBs on mobile device. This technology provides encryption standards needed for application data either at compile time or via wrapping technology. All data stored by the application is stored in a secure container that encrypts both files and embedded SQL technology on the devices.
- Further these applications can have their network access controls managed by the solution to ensure network connections are routed appropriately through secure SSL channels based on application, domain name, etc.
- Enterprise isolation from other user own apps on device: Each application can receive its own SSL encrypted tunnel that can only be leveraged by that application.
- Inherit all MDX security features: SSO, secure inter-app communication, information/data containment, restrictions based on device states.

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 both iOS and Android systems.

It should be noted that it is not legal per Apple's terms to wrap an application that has been signed and published to a public app store. Wrapping such applications requires assistance from the respective developer(s).

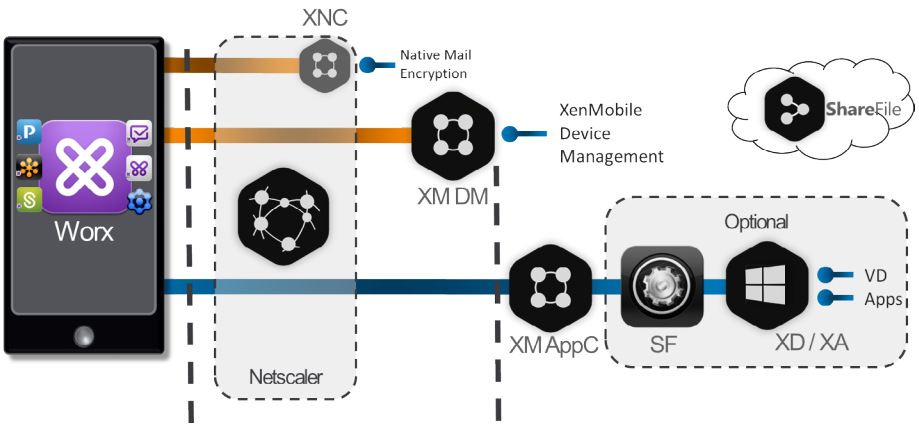
This produces challenges for IT, as there are a number off the shelf applications that would be suitable for business use yet need IT controls. For this reason, Citrix has partnered with many application developers to provide off the shelf, Citrix enabled applications.

As of this writing there are over 85 applications in the Worx Enabled Partners store - no other vendor has this level of support and participation in their MAM arsenal.

Applications prepared via compile time or app wrapping provide built-in facilities 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 a 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



Component description

For the purposes of this document, the following components could be considered in a XenMobile deployment. There are very few interdependencies between components, and some components may be combined in a single server installation.

Component	Deployment method	Description
Client components		
Enroll application	Public application store, pushed	Pushed/pulled via enterprise app store
Worx Home	Public application store, pushed	MDM/content management/ jailbreak detection/GoToAssist functionality.
WorxMail™	Pushed/pulled via enterprise app store	Sandboxed/policy-wrappable secure mail/ contacts/calendar client for MS Exchange. Available on iOS and Android, presently.
WorxWeb™	Pushed/pulled via enterprise app store	Sanboxed/policy-wrappable secure web browser application, available on iOS and Android, presently.
Gateway zone components		
Netscaler	Virtual or physical appliance	Application delivery server/ NetScaler Gateway/load balancer.
XMDM server	Physical installation	MDM policy management server.
XNC	Physical installation, can be installed on XMDM Server	Optional enforcement at gateway for non-compliant devices.
Enterprise zone components		
App Controller	Virtual appliance	Policy management for MAM/SSO web apps.
StoreFront	Physical installation	Optional consolidation server for enterprise app store when combining existing XenApp®/XenDesktop® services.
XM Mail Manager	Physical installation	Optional mobile service to control discovery and enforcement of exchange.

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 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

The core components of NetScaler Gateway are:

Virtual servers

The NetScaler Gateway virtual server is an internal entity that is a representative of all the configured services available to users. The virtual server is also the access point through which users access these services. You can configure multiple virtual servers on a single appliance, allowing one NetScaler Gateway appliance to serve multiple user communities with differing authentication and resource access requirements.

Authentication, authorization, and accounting

You can configure authentication, authorization, and accounting to allow users to log on to Gateway with credentials that either Gateway or authentication servers located in the secure network, such as LDAP or RADIUS, recognize. 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.

User connections

Users can log on to NetScaler Gateway by using the following access methods:

- The NetScaler Gateway Plug-in for Windows is software that is installed on the user device. Users log on by right-clicking an icon in the notification area on a Windows-based computer. If users are using a computer in which the NetScaler Gateway Plug-in is not installed, they can log on by using a web browser to download and install the plug-in. If users have Citrix Receiver™ and/or Worx Home installed, users log on with the NetScaler Gateway Plug-in from Receiver/Worx Home. When Worx Home and the NetScaler Gateway Plug-in are installed on the user device, Worx Home starts the NetScaler Gateway Plug-in automatically.
- The NetScaler Gateway plug-in for Mac OS X that allows users running Mac OS X to log on. It has the same features and functions as the NetScaler Gateway plug-in for Windows.
- The NetScaler Gateway plug-in for Java that enables Mac OS X, Linux, and optionally, Windows users to log on by using a web browser.
- Worx Home that allows user connections to published applications (native device and Windows-based) and virtual desktops. Users can also connect to web and SaaS applications, iOS mobile apps, and ShareFile data hosted in App Controller.

When configuring NetScaler Gateway, you can create policies to configure how users log on. You can also restrict user logon by creating session and endpoint analysis policies.

Network resources

These include all network services that users access through NetScaler Gateway, such as file servers, applications, and websites. The NetScaler Gateway can provide transparent sign-on to network resources using HTTP Basic, Digest, NTLM, Kerberos and Form-Fill.

Virtual adapter

The NetScaler Gateway virtual adapter provides support for applications that require IP spoofing. The virtual adapter is installed on the user device when the NetScaler Gateway Plug-in is installed. When users connect to the internal network, the outbound connection between NetScaler Gateway and internal servers use the intranet IP address as the source IP address. The NetScaler Gateway Plug-in receives this IP address from the server as part of the configuration.

If you enable split tunneling on NetScaler Gateway, all intranet traffic is routed through the virtual adapter. Network traffic that is not bound for the internal network is routed through the network adapter installed on the user device. Internet and private local area network (LAN) connections remain open and connected. If you disable split tunneling, all connections are routed through the virtual adapter. Any existing connections are disconnected and the user needs to reestablish the session.

If you configure an intranet IP address, traffic to the internal network is spoofed with the intranet IP address through the virtual adapter.

Device Manager (MDM)

XenMobile Device Manager allows you to manage mobile devices, set mobile policies and compliance rules, gain visibility to the mobile network, provide control over mobile apps and data, and shield 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 like PKI and Security Information and Event Management (SIEM) systems, Device Manager simplifies the management of mobile devices.

You can use XenMobile Device Manager to manage iOS, Android, Windows 8 and Windows Phone 8, Windows Mobile, and Symbian mobile devices. With the Device Manager 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, configure access controls, set application blacklist and whitelists, configure an email server, locate devices, remotely wipe lost or stolen devices, and configure advanced PKI certificates or SAML authentication.

Device Manager contains the following features:

- Ability to enroll mobile devices
- Capability to automatically deploy device management configurations on mobile devices that includes:
    - Policies (security policies, restrictions, device configurations and settings etc)
    - Software packages / App delivery
    - Registry keys / XML configuration files
    - Files
    - Scripts
- Deployment of packages for devices, users, and groups with the capability to restrict deployment based on comprehensive rules and scheduling.

- Central visibility and auditing which includes.
  - User and device management configurations and settings
  - Device hardware and software inventory
  - Connection logs
- High availability and scalability that provides consistent availability by using a multi-server redundant architecture and load balancing supporting very large deployments
- Remote control, remote lock/unlock, remove selective wipe, remote device wipe etc.
- Role-based administration and delegation
- Online mobile activity reports, providing detailed information on user / devices / policies / deployment packages

App Controller (MAM)

App Controller provides access to web, SaaS, mobile apps, and ShareFile. This component allows IT to protect enterprise apps and data with policy-based controls, such as restriction of application 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 Worx Home.

With App Controller, you can provide the following benefits for each application type:

- SaaS applications: Active Directory-based user identity creation and management, with SAML-based single sign-on (SSO)
- Intranet web applications: HTTP form-based SSO by using password storage
- iOS and Android native applications: Unified store to which you can install MDX applications, and security management for MDX policies, encompassing WorxMail and WorxWeb
- ShareFile access: Integrated enterprise data access with synchronization with Worx Home, seamless SAML SSO, and Active Directory-based ShareFile service user account management

App Controller enables the delivery of web, SaaS, Android- and iOS-based applications, and ShareFile data, along with Windows-based applications from XenApp and virtual desktops from XenDesktop. You manage web, SaaS, Android- and iOS-based application configuration and policy settings by using App Controller, with the following capabilities:

- Centralized user account creation and management for web and SaaS applications, and ShareFile access that provides users with a seamless single sign-on (SSO) experience.
- The use of Active Directory as the identity repository. Active Directory is then used as the basis for authorizing users to external applications and services.
- A unified enterprise app store to enable the publishing and distribution of Android- and iOS-based applications for authorized users to download and install on mobile devices.
- Centralized policy controls to secure the 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.

You can configure applications and ShareFile access by using the App Controller web-based management console. Within the management console, you can configure the following:

- Roles that include Active Directory groups
- Applications for SSO only
- Applications for SSO, user account management, and the creation of new user accounts
- Applications for Android and iOS devices, including WorxMail™ and WorxWeb™ applications
- Approval workflows for creating user accounts
- Categories to organize applications in Citrix Worx Home
- HTTP Federated Formfill connectors
- SAML 1.1 or 2.0 connectors that support the identity provider (IdP) flow
- Role-based management and delivery of mobile applications
- Role-based ShareFile document management with support for Storage Zones
- Device inventory that lists user devices that connect to App Controller

Key Features

The most typical deployment configuration for App Controller is to locate App Controller in the secure network. Users can connect to App Controller to access applications, as well as ShareFile data and documents.

The key features of App Controller are:

- Access to web and SaaS applications that includes:
  - Federated support for SAML 1.1 and SAML 2.0 applications
  - Password storage and formfill support for password-based web applications
  - User account management from Active Directory group membership for SaaS applications
  - User account management workflows that allow users to request application accounts and for individuals in your organization to approve the requests
- Access to Android and iOS mobile applications that includes:
  - The ability to publish Android and iOS applications that users can download and install on their mobile devices from Citrix Worx Home, including WorxMail and WorxWeb
  - Security controls for Android and iOS applications which provide application and data security
  - Management of mobile applications on user devices through Worx Home which enables you to control the mobile applications without managing the mobile device
- Access to ShareFile that includes:
  - Creation and deletion of user accounts within ShareFile by using Active Directory rules
  - Choice of storage location per folder: ShareFile-managed cloud storage or an on-premises Storage Zone, enabling you to optimize performance and address data sovereignty and compliance requirements
  - Centralized device listing for users that allows you to erase application and ShareFile data on lost or stolen devices
- Device inventory that includes:
  - The ability to view all devices that have connected to App Controller
  - The ability to erase and stop erasing data on the user device
  - The ability to lock and unlock the user device
  - The ability to remove devices from the list

Citrix productivity apps: WorxMail and WorxWeb

People want and expect to be able to work when and where they need to, on any device. And increasingly, the focus is on the apps. But the app revolution has serious implications for enterprise IT when it comes to security and compliance. For many organizations the risk of a rogue or questionable app has resulted in a policy of "no". A blocked app can cause a lot of frustration and paralyze the productivity gains everyone expects from mobile. To address this challenge, Citrix and its partners in the app development community have created Worx Mobile Apps.

With Worx Mobile Apps, any developer or administrator can add enterprise capabilities, such as data encryption, password authentication or an application-specific micro VPN. IT can find Worx-enabled apps in the Worx App Gallery and developers can use the App Gallery to promote their apps.

WorxMail

WorxMail is a native iOS and Android email, calendar and contacts app. Citrix WorxMail integrates with other Worx Mobile Apps and leverages the mobile app security features in XenMobile through MDX technologies to offer secure productivity on the go. Users can attach docs to emails and save attachments back using ShareFile, open attachments and web links, including internal sites, with WorxWeb, and view the free/busy information of colleagues before sending a meeting invite, all while staying inside the secure container on the mobile device. WorxMail supports ActiveSync and Exchange and offers security features, such as encryption, for email, attachments and contacts.

WorxWeb

WorxWeb is a mobile browser for iOS and Android devices that enables secure access to internal corporate web, external SaaS, and HTML5 web applications while maintaining the look and feel of the native device browser. WorxWeb leverages MDX technologies to create a dedicated VPN tunnel for accessing a company's internal network and the other MDX security features to ensure that users can access all of their websites, including those with sensitive information. WorxWeb offers a seamless user experience in its integration with WorxMail to allow users to click on links, such as 'mailto' and have the native apps open inside the secure container on the mobile device.

Worx Home

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

Worx Home 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.

Worx Home serves as the encryption key broker for all MDX, Worx-enabled applications. Each application under management retrieves its policy check-in times from the Worx Home application. The applications will then verify timers across each application/resource on the device. When a user is successfully authenticated, an application specific key is generated with an

associated expiration time applied. 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 and security

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 App Controller Appliance.

App Controller is a virtual appliance that provides Citrix specific application management and policy control for MDX based applications. The App Controller 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.

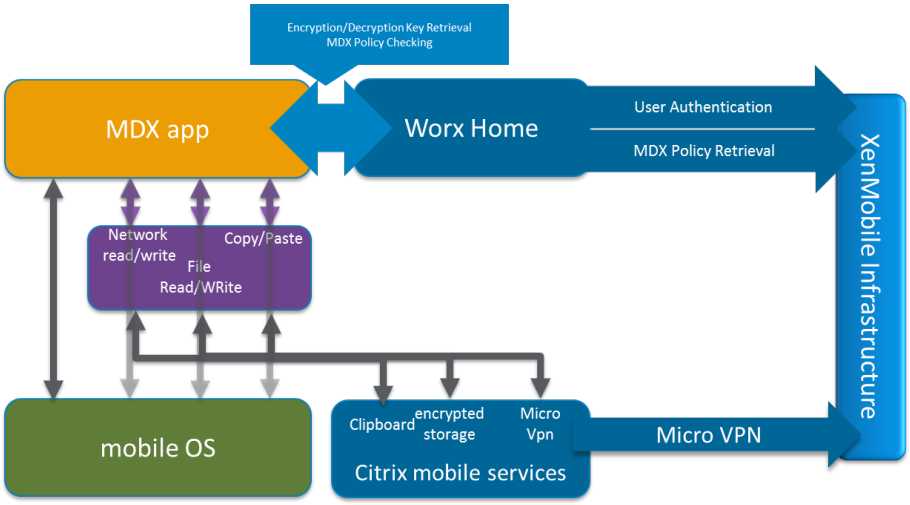
The App Controller then generates strong cryptographic random numbers which are then encrypted and sent via SSL tunnel back to the device.

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. Worx Home protects these variables in its encrypted keychain for later use as needed.

The server provided random numbers, the DeviceID, and other unique values are used in the AES key generation.

Worx Home utilizes these cryptographically strong variables to generate an AES encryption key. The encryption key on iOS is an AES-256 bit key. The encryption key on Android is an AES-128 bit key

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



Device data at rest – At a glance

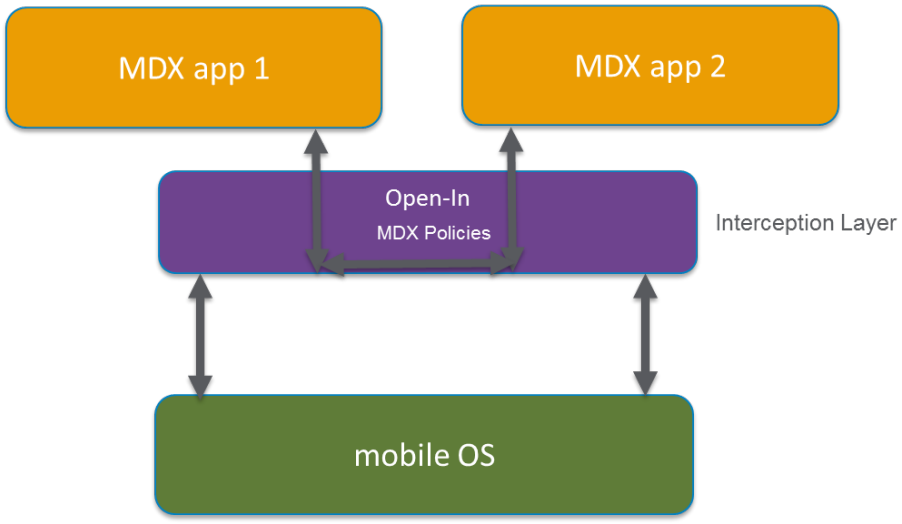
Platform	Location	Strength	Key location
iOS	Native OS	AES-256	Based on device password, stored on keychain DB
	MDX applications	AES-256	AES-256
Android	Native OS	AES-128	
	MDX applications	AES-256	

How is my data protected at rest?

Most employees today do their best to protect company interest. But sometimes, employees use unsanctioned and insecure tools for work. This often rears its head in the form of users leveraging application and cloud storage systems that are not under company control, or copy/paste content into unprotected email systems. These applications make the mobile life of the end user more productive, but are provided at the expense of losing control of the data. The opposite end of the spectrum comes in the form of the malicious user attempting to steal company data. Regardless of the motive, IT needs tools to protect the 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 such that opening documents can only be performed in company wrapped applications. So when an employee receives an email with an attachment, only those apps approved by the company are available for use. Even links to web sites can be forced to open in a secure browser.
- Only allow use when on company network:
  - Application level policies (copy/paste/network access/etc.)
  - Interapp access controls (open-in, etc.) – outlined below in a functional diagram



How is my data protected in transit?

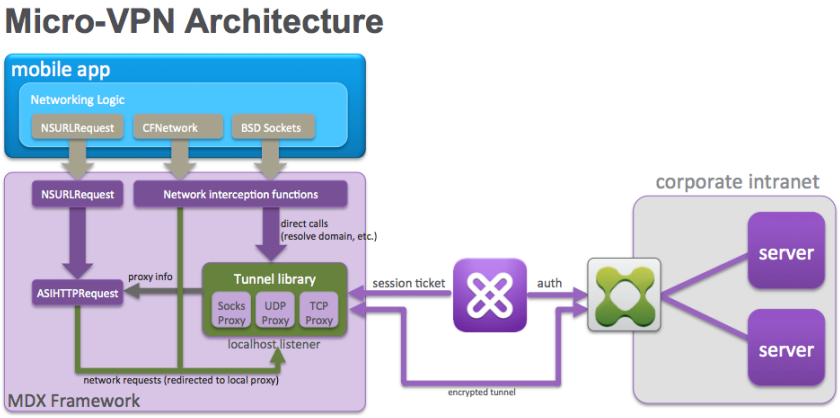
Micro-VPN

A core feature of the MDX framework is Micro-VPN capability, allowing 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)

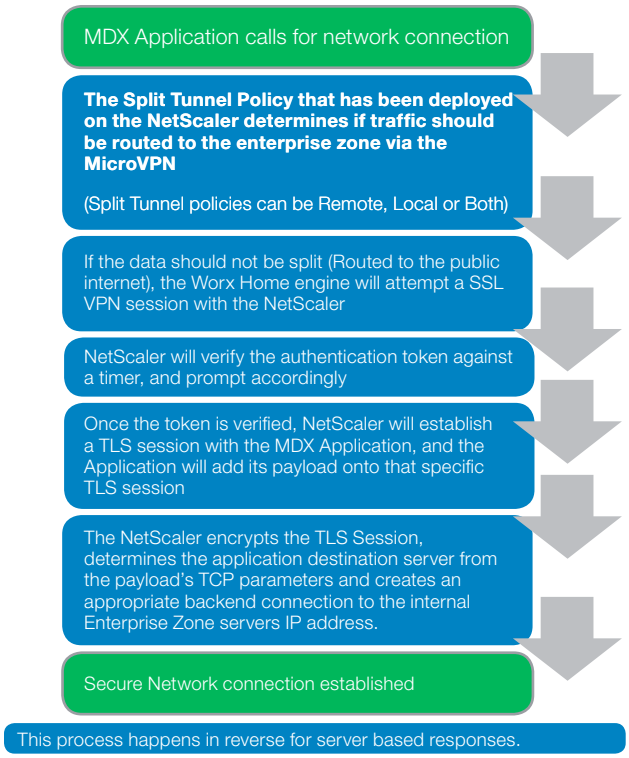
Micro-VPN tunnels are unique per-application and encrypted to be protected from other device communication or other Micro-VPN communication.

In addition to security features, Micro-VPNs also offer data optimization techniques including compression algorithms to ensure A) only minimal data is transferred and B) this is done in the quickest time possible, improving user experience – a key success factor in mobile project success



Data flow of a typical Micro-VPN connection

The following diagram outlines a typical network call established as part of the MDX policy definition within App Controller. Although App Controller will define usage of a Micro-VPN, the NetScaler will ultimately determine the path the client takes once it hits the gateway.



Encryption level for TLS session

Can be defined on the NetScaler, but is typically AES-256.

How is my data protected at HQ?

Security inside the company network is just as critical if not more so than on the mobile device. Citrix takes a number of measures to protect the mobile management infrastructure. The primary components of a XenMobile solution include NetScaler (Gateway), App Controller and Device Manager. Standard security penetration testing is done to ensure no exposed attack vector exists.

NetScaler provides a secure application firewall. NetScaler serves as the primary edge 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.

XDM leverages a hardened Tomcat web services deployment customized for MDM management.

Database services are provided by Microsoft SQL Server or Postgres (eval/testing only). XDM is logically separated from the database. Database can reside anywhere. Best practice is to install the database inside the company network. Thus critical data, regardless of state, is not sitting in the DMZ.

Authentication of users is provided by LDAP services in a real-time manner. This reduces the amount of data that must be stored in the XDM system and reduces potential exposure.

Internal controls

Citrix have an independent security team, that is not part of the code development group. This group evaluates the product software, much like an external entity would, and flags security concerns, that are prioritized across severity levels of critical, high, medium and low. The engineering teams are expected to respond back to the raised concerns – with fix schedules, before the product is certified ready for release.

NetScaler

NetScaler / firewall configuration file of device is on protected disk storage of the physical or virtual appliance. All administrative access to the device is controlled via authentication using the AAA subsystem, which supports locally defined users and users in AD, other LDAP directories or TACACS+.

XMDM

Configuration is stored in the database, either onboard or external SQL server. Access is protected via authentication.

App Controller

Configuration is stored in the onboard database. Access is protected via authentication using a local administrator account. Access is limited to basic commands on the system. Full root access is not permitted.

Worx Mobile Apps

All configuration is stored within the app with encryption. Users have a UI to edit certain parameters and is accessible only upon authentication.

Citrix Receiver and Worx Home

Receiver and Worx Home stores only the configuration of the Citrix store FQDN that it needs to communicate with.

Embedded PKI

Cryptography

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

Critical data needed to run at the device and server levels is encrypted using AES-256 encryption. An example would be 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 secure in files and the database in AES-256 format.

Device / Server verification (how we know device is who it says it is)

XenMobile employs strong two-factor authentication to prevent possible attacks. Multiple levels of digital certificates have formed the foundation of XenMobile security infrastructure. A device certificate is issued during the enrollment process and is required for communications between a device and XenMobile servers.

iOS enrollment initiated installation of the Worx enrollment client signed and approved by Apple for the App Store.

Jailbreak status is validated prior to enrollment. On iOS, enrollment starts with device certificate request using SCEP protocol via the built-in MDM capabilities embedded in the iOS operating system. Devices certificates are signed and issued by either embedded XenMobile Certificate Authority (CA) or 3rd-party trusted CA e.g. when customer already has a PKI deployment in place. XenMobile supports most of the popular commercial CA services, such as Microsoft, Symantec, RSA, and OpenTrust CA. These certificates are used in communication to ensure the device is who it says it is. From this point forward basic device management is performed by authenticating the client with the appropriate certificate handshakes.

Android enrollment is initiated via the Worx enrollment client published on the Google Play or Amazon Kindle App stores. Basic user authentication is performed as explained above. Device is evaluated for rooted status, then allowed to authenticate. Once completed, certificates are exchanged. These certificates are passed from this point forward to authenticate the client to XDM solution.

All data and certificates/private keys locally stored on the device are encrypted using AES-256 encryption or strong platform native service such as iOS keychain. URLs can be used by the enrollment process to reduce the attack surface of the server exposed to the internet.

User enrollment

Device enrollment

There are basic differences between iOS and other managed platforms for enrollment, the process of joining a device to the managed service, mostly due to the direction and APIs offered by the device manufacturer.

There are a number of optional enrollment options within XenMobile MDM, to give a balance between security and usability. These include:

A username (locally created or active directory)

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
An enrollment URL	Random unique URL that must be used on the XDM server

In addition - each device enrollment may have the following attributes associated:

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 passing validity from a SAML server such as Active Directory Federated Services (ADFS).

APNS

APNS is an Apple specific notification method and service for secure notification of both "connect" events for MDM and general device notifications (message popups). APNS ensures only valid messages get pushed to devices, and all MDM activity is associated with a server installed certificate that is co-signed by a MDM provider.

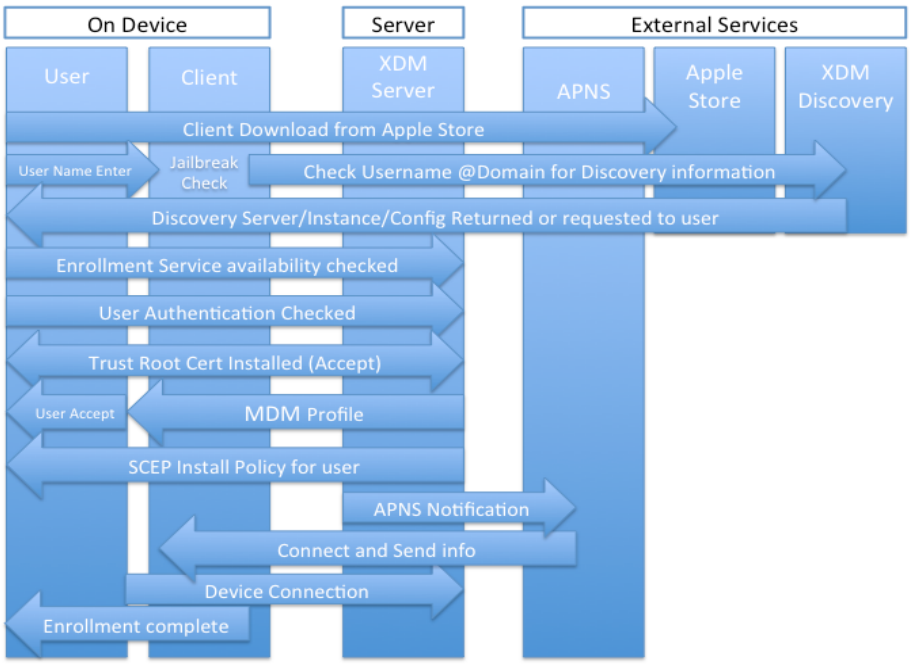
For a further detailed description of APNS, and its capabilities, Apple has further information at:

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

iOS initial enrollment flow

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:



During enrollment, the user is prompted to enter a username or email address that will be used to identify within the service.

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

The XDM enrollment service is checked for availability and the user is authenticated against the XDM server, as well as confirming the device has not been revoked previously. The XDM server will use either local (database) or active directory authentication to confirm 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.

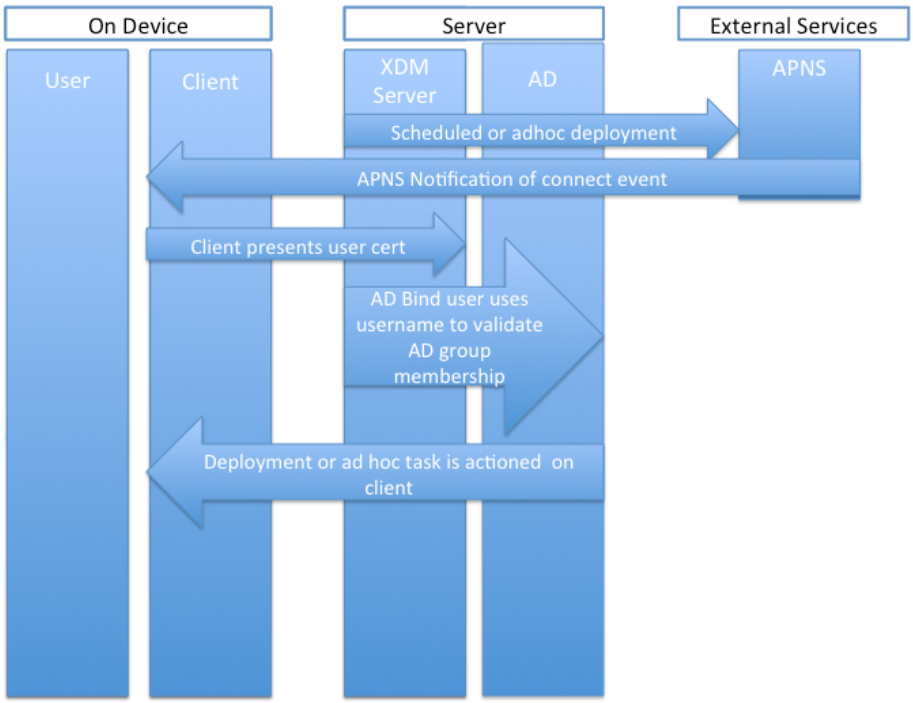
Post-successful authentication an optional terms and conditions will be presented. If a user denies this, they can no longer continue enrollment.

If the server has self signed the root certificate, the user will then be prompted to accept a root to set up the enrollment of the device – an alternative would be to install a trusted certificate on the XDM server.

At enrollment, a certificate is generated and installed on the client to represent the user for future MDM sessions.

Once SCEP is complete, the XDM server instructs the APNS to notify the device to use the cert to connect in to the standard XenMobile connection port to complete the enrollment, and run the initial DM session, collect inventory etc.

Post enrollment (day to day connectivity)



Day to day management takes place in one of the 4 scenarios below:

- A scheduled deployment – where a deployment task is delayed until a specific time
- A scheduled inbound check-in – by default every 6 hours for iOS, this is configurable
- An adhoc task, such as right click lock/wipe/locate, actioned by a console administrator
- Via a web service call

All events are triggered via an Apple push notification instructing the device to connect inbound over port 443.

When a device connects inbound to the XDM service, it presents a valid certificate containing the user ID of the device. This ID is used by the AD bind user to check three attributes:

- AD group membership
- User account is not disabled
- AD attributes of 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 AD Bind user.

Secondary service connections

In addition to the certificate based primary authentication, secondary authentication such as forms-based authentication may be required for access to SharePoint.

At present this will require a user to add additional credentials in a pop up box.

These credentials are passed via the SSL cert secured tunnel to the requester, and stored encrypted locally until the server policy defines that they should be expired.

Additional security features

IT automation

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 approved applications and processes – this prevents both installation and execution of unauthorized tasks.

Typical use cases might be preventing access to public application stores, restricting leisure applications or simply preventing configuration change.

This is achieved with a task watcher embedded into the client – able to prevent interaction with any unauthorized execution.

Web services

Because today's enterprise demands 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 XMDM server. This approach has also been a key differentiator when working with our service provider partners to offering billing integration and access from a unified portal.

Automated actions

Any solution should provide automated actions to protect and inform the user and security admin in the event of an issue. An automated action can be considered to be 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 unenrollment process and drives security based on IT existing best practices.

This process should not only remove the user from access to company systems, but also remove company apps, follow me data (cloud storage), cloud systems (SFDC, etc.) along with SSO credentials, etc.

These actions may be combined and may result in notifications/blocking/flagging as out of compliance or wiping – the enterprise has the flexibility to make this choice.

Auditing capabilities

XenMobile leverages industry recognized controls for maintaining Security Information and Event Management (SIEM) data – in addition to audit trails of server based activity, key user information can be gathered from the gateway components, including time of access, IP address and device data.

NetScaler

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

XMDM

Audit trails are stored in the central XMDM database, and Citrix XMDM provides out-of-the-box audit trail reports, which includes user info, activity info, date/time stamps etc for administrative actions etc. XMDM does not (by default) expire audit trails/info from the database. Citrix provides different levels of server logging, and verbose logging is mainly used if needed during troubleshooting exercises. No data is shown in log files, however log files will contain user information (such as logon UserID with no password information). Many device policy violations (e.g. jailbreak, unmanaged device, location perimeter violation, location disabling etc.) can be configured to generate automatic alerts. Application, device, user login events all are recorded in audit logs. Different levels of logs/audits (info, warning, errors) or per-module can all be configured. The information is available for access via SNMP.

App Controller

Rich audit trails recorded both on the appliance, as well as streamed to configured external log collection servers.

Denial of service protection

NetScaler

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

XMDM

Standard security penetration testing done to ensure no exposed attack vectors exist. Additional app firewalling is possible via NetScaler.

App Controller

Standard security penetration testing done to ensure no exposed attack vectors exist. Additional app firewalling is possible via NetScaler.

Citrix Worx Home

Our common SDL practices dictate 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 do any explicit input or sanity checking on the incoming data from NetScaler or other enterprise resources such as Exchange. We trust that the server is sending us a valid stream.

PKI integration and distribution

XDM can make certificate requests to external certificate service providers such as Microsoft, Entrust 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 to devices but only those that are compliant with company security and compliance needs. Certificates can provide access to network resources without the need for user interaction, or serve 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 SCEP (Simple Certificate Enrollment Protocol).

Certificate revocation and renewal are also catered for driving a balance between security and usability.

References and appendices

XenMobile Worx MDX-enabled applications

An enterprise can use one of three ways to obtain Worx-enabled applications

- Application wrapping of an existing mobile application
- 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 apps.
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.
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 for one application to pass requests for help to another. This policy serves to filter the schemes that are actually passed into this application for handling (that is, inbound URLs).
Allowed URLs	This policy serves to filter the URLs that are passed from this application to other applications for handling (that is, outbound URLs).

Specific restrictions at a Worx enabled application level:

Application specific policy	
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:

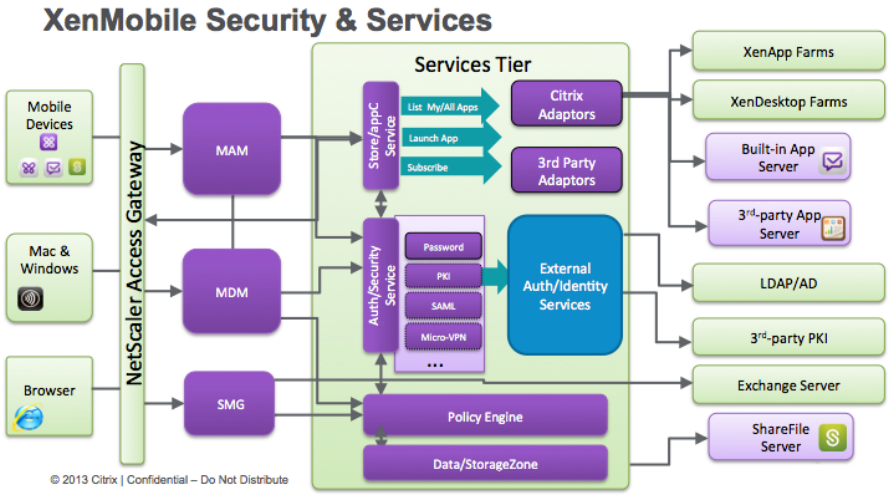
Security settings	
Block jailbroken and rooted devices	When set to On, the application is locked when the device is jailbroken or rooted. If Off, the application can run even if the device is jailbroken or rooted.
Enable database encryption	When set to On, this policy ensures that the data held in local 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 each time they are needed from the key management service of XenMobile. When Offline access permitted is selected, secrets used to derive encryption keys may persist on the device. When set to Online access only, then the Authentication policy is assumed to be "Network logon required" regardless of the authentication policy setting that is actually configured for this 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 to protect access to the keys and associated encrypted content.

Erase app data on lock	When set to On, when an application is locked, any persistent data maintained by the app is erased, effectively resetting the app 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 Worx Home account removed, Citrix Worx Home uninstalled, too many app authentication failures, jailbroken or rooted device detected without policy permitting app 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 XenMobile in an attempt to determine current application and device status. Assuming XenMobile 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 on. Whether XenMobile is reachable or not, a subsequent poll will be scheduled based on this interval. After this period expires, a new poll will be attempted.

And 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 the network access. If Blocked, all network access is blocked. If Tunneled 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 App Controller beacons. If Off, the app can run from an external network as well.
Require Wifi	When set to On, the app is locked when the device is not connected to a Wifi network. If Off, the app can run even if the device does not have an active Wifi connection such as 4G/3G or a LAN 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



Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

CITRIX®

About Citrix
Citrix (NASDAQ:CTXS) is a leader in mobile workspaces, providing virtualization, mobility management, networking and cloud services to enable new ways to work better. Citrix solutions power business mobility through secure, personal workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive. With annual revenue in 2013 of $2.9 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