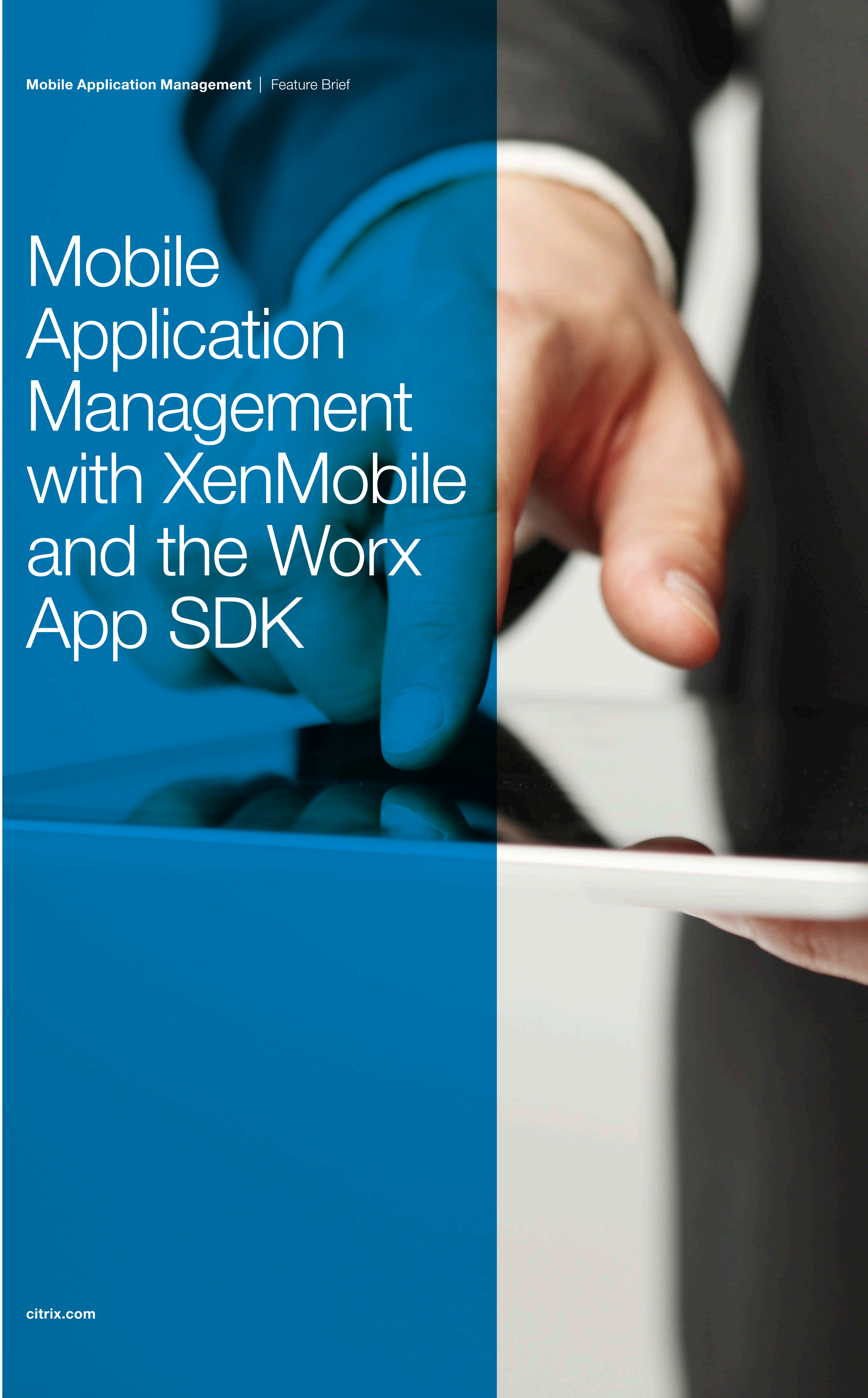
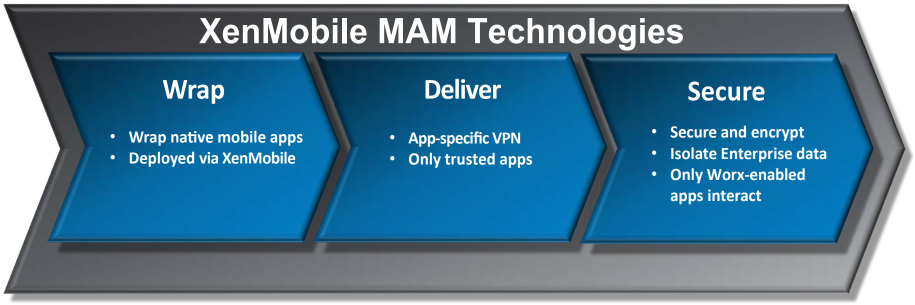


Mobile Application Management with XenMobile and the Worx App SDK

Enterprises of every size and across every industry have made mobility an important IT initiative. While most mobility strategies started with mobile device management to address the device lifecycle needs of bring-your-own (BYO) or corporate-owned mobile devices, organizations are now expanding their plans to address mobile application lifecycle and mobile application performance. While BYOD programs make employees happier and more productive, many organizations are counting on the increased business efficiency, competitiveness and top-line gains they can realize from truly mobilizing their workers. Enterprise mobile applications and mobile data management are at the heart of such enterprise mobility programs.

It's all about the apps

Consumer apps are quickly moving into the enterprise. Furthermore, enterprises are developing and adopting in-house mobile apps that change the way they do business. These range from productivity apps such as Evernote and QuickOffice to purpose-built applications to optimize the guest check-in process at restaurants, control the logistics of pilot scheduling at air freight companies or reduce customer wait times through quicker valet vehicle retrievals at luxury hotels. The mobile information management capabilities afforded by such enterprise apps are giving businesses new ways to take advantage of corporate data and achieve greater operational efficiencies.


XenMobile MAM Technologies
Wrap
• Wrap native mobile apps
• Deployed via XenMobile
Deliver
• App-specific VPN
• Only trusted apps
Secure
• Secure and encrypt
• Isolate Enterprise data
• Only Worx-enabled apps interact

The power of the Worx App SDK

The mobile application management (MAM) capabilities in Citrix XenMobile enable complete management, security and control over native mobile apps and their associated data. The Worx App SDK, a simple and powerful SDK that Worx-enables any mobile app, leverages Citrix MDX app container technology to separate corporate apps and data from personal apps and data on the user's mobile device. This allows IT to secure any custom developed, third-party or BYO mobile app with comprehensive policy-based controls, including mobile DLP and the ability to remote lock, wipe and encrypt apps and data.

Using the Worx App SDK, IT can:

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

In this paper, you will learn about the Citrix mobile application management capabilities in XenMobile and how to use them to secure and manage your native mobile apps and data.

Worx App SDK with MDX for secure access

MDX provides the industry's first application-specific VPN access to a company's internal network via the Citrix NetScaler Gateway feature. When a user tries to access a company's internal network remotely, an app-specific VPN tunnel is created just for the mobile apps in use.

Consider the situation where an employee wants to access the following resources within the secure enterprise network from a mobile device: the corporate email server, an SSL-enabled web application hosted on the corporate intranet and documents stored on a file server or Microsoft® SharePoint®. MDX enables access to all these enterprise resources from any device through an application-specific micro VPN. Each of these apps is provided with its own dedicated micro VPN tunnel.

Micro VPN functionality does not require a device-wide VPN that can compromise security on untrusted mobile devices. As a result, the internal network is not exposed to viruses or malware that could infect the entire corporate system, and corporate mobile apps and personal mobile apps are able to co-exist on one device. MDX with micro VPN technology fills a significant gap left by traditional secure remote access technologies.

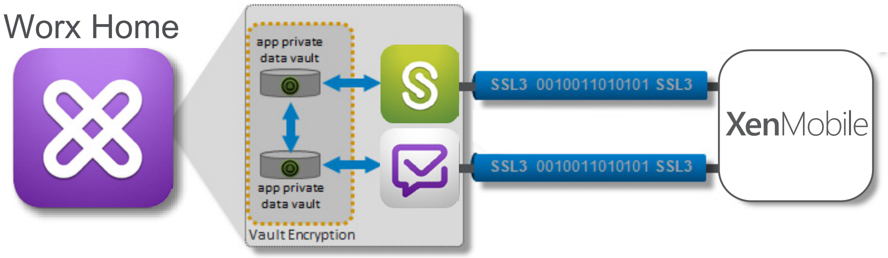


Figure 1. MDX provides policy-based management and access controls over all app types.

MDX access policies

MDX Technologies enable IT to require strong authentication and endpoint analysis before even permitting users to download and install applications on their devices. Once these apps are installed, Worx Home, a mobile app that provides access to desktops, apps and data, ensures that the desired policies are continuously enforced, always keeping IT in control of the enterprise content on users' devices. Additionally, with MDX policies working in conjunction with the Citrix WorxWeb secure browser, IT can control how the application traffic is routed: the application can use either the micro VPN tunnel (to access resources within the corporate network) or the device's network connection (to access SaaS applications hosted by a third party).

Figure 2 provides a screenshot and a description of each of the security policies that can be applied to any mobile application delivered through XenMobile.

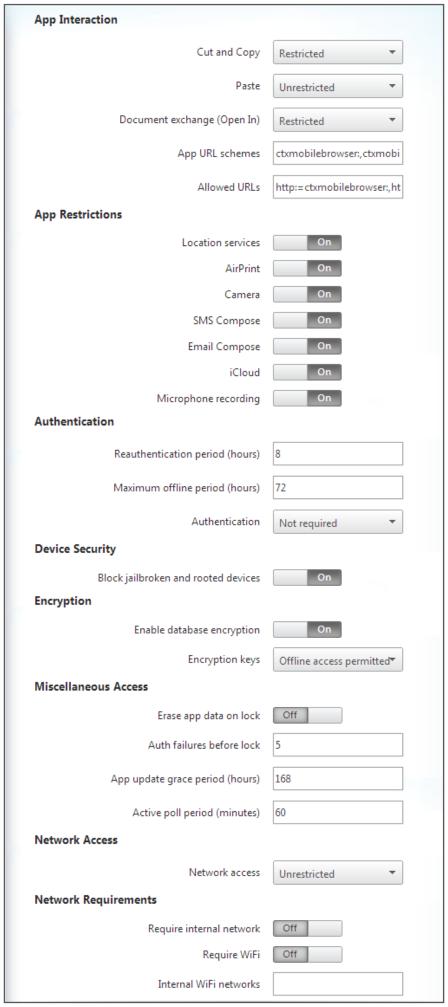
App interaction

- **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 Worx-enabled 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 Worx-enabled apps.

- **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 Worx-enabled apps.

- **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).



App Interaction	
Cut and Copy	Restricted
Paste	Unrestricted
Document exchange (Open In)	Restricted
App URL schemes	ctxmobilebrowser:,ctxmobi
Allowed URLs	http:=ctxmobilebrowser:,ht
App Restrictions	
Location services	On
AirPrint	On
Camera	On
SMS Compose	On
Email Compose	On
iCloud	On
Microphone recording	On
Authentication	
Reauthentication period (hours)	8
Maximum offline period (hours)	72
Authentication	Not required
Device Security	
Block jailbroken and rooted devices	On
Encryption	
Enable database encryption	On
Encryption keys	Offline access permitted
Miscellaneous Access	
Erase app data on lock	Off
Auth failures before lock	5
App update grace period (hours)	168
Active poll period (minutes)	60
Network Access	
Network access	Unrestricted
Network Requirements	
Require internal network	Off
Require WiFi	Off
Internal WiFi networks	

Figure 2.

- **Allowed URLs**
  iOS applications can dispatch URL requests to other applications that have been registered to handle specific schemes (such as "http://"). This facility provides a mechanism for an application to pass requests for help to another application. This policy serves to filter the URLs that are passed from this application to other applications for handling (that is, *outbound* URLs).

App 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

- **Reauthentication 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.

- **Authentication**
  - **Enterprise logon required**
    The app requires the user to log on and will permit online usage only
  - **Offline access permitted after challenge**
    The app prompts the user to log on but allows offline usage after PIN/passcode/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

Device security

- **Black 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.

  This policy determines whether an application will be allowed to run on a jailbroken device.

Encryption

- **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 for **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.

Miscellaneous access

- **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, 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.

Network access

- **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 per-application VPN tunnel back to the internal network is used for all network access.

Network requirements

- **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 XenMobile 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 **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.

  Here, you provide a list of SSIDs representing trusted internal network names and the application will only be allowed to launch if the device is connected to one of the defined wireless networks.

Worx App SDK with MDX for secure app containers

The MDX secure mobile container technology separates and isolates mobile business applications and data from personal content on any mobile device. Now, IT can remotely manage, control, lock and wipe critical Worx-enabled, business applications and data without touching the employee's personal content or device.

To create a complete, secure container using MDX, three additional technology pieces should be used:

1) Work Home, an app that allows IT to enforce mobile settings and security. Employees use this app to access their unified app store and live support services. XenMobile communicates with Worx Home to deliver MDM and Worx-enabled app policies.

2) Native mobile apps that have been Worx-enabled with the Worx App SDK are published to the XenMobile App Controller component of XenMobile.

3) For mobile data management and control, Citrix XenMobile includes ShareFile, which secures corporate data on the device.

Mobile apps: locally installed while fully controlled

To manage native mobile applications, over-the-air distribution files (.ipa files for iOS or .apk files for Android) must be "Worx-enabled" using the Worx App SDK. With a single line of code or generic wrapper, any developer or administrator can add enterprise capabilities to a mobile app. Once complete, security and usage policies are applied to each individual mobile app.

Policies can include preventing the user from taking screenshots, copying and pasting content, requiring the mobile device to be connected to a secure wireless network / denying access to content while connected via a cellular network, forcing authentication at every app launch, disabling iCloud for app backup, disabling content being sent via SMS or native email for a secured application and disabling the camera.

In preparation for app distribution to mobile devices, the Worx-enabled applications are uploaded to XenMobile. These Worx-enabled apps are then containerized with MDX. To prevent unauthorized usage, access rights to each application are managed by assigning user groups from Microsoft® Active Directory® to the application. Applications will not be visible to any user who is not part of the Active Directory user group(s) authorized within XenMobile to use the specified application.

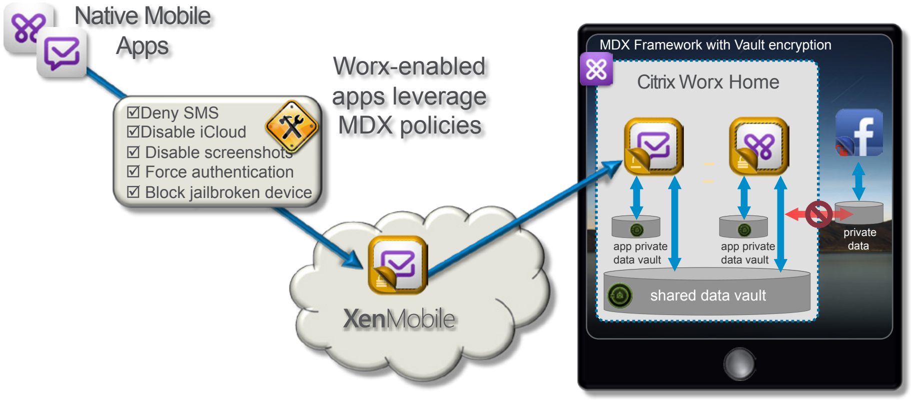


Figure 3. MDX keeps corporate applications and data separate from personal apps in a secure container.

Worx Home enables users to subscribe to any application for which they are authorized based on their role. These applications are then deployed from XenMobile into a secure container enabled by MDX on the mobile device. These secure containers are invisible to employees, who can seamlessly exit the application to use their own consumer apps without risking data leakage.

In addition to mobile application management, IT can manage and secure mobile data using ShareFile. ShareFile gives people secure access to files on their device of choice while giving IT complete security and control over corporate data. To deploy a shared secure container for both apps and data and allow seamless interaction between ShareFile docs and native mobile apps such as Citrix WorxMail, IT must deliver ShareFile using XenMobile. Downloaded files as well as locally installed apps are secured “at rest” on the device using AES 256-level encryption. Data in motion is secured with SSL 3 encryption. In this container, IT can apply the following comprehensive policy-based controls over corporate data:

- Mobile data leakage prevention (DLP)
    - Disable copy/paste
    - Disable iCloud
    - Disable “Open In” functionality
    - Disable emailing of corporate docs
- AES 256 encryption when data is at rest and SSL 3 encryption when data is in motion
- Mobile application management enforcement, such as store logon requirement, device requirements, network requirements
- Lock and wipe apps and data remotely
- Mobilization of any iOS or Android app
- App and data control via policies
- Open attachments only with Worx-enabled apps

- Enable Worx-enabled apps to seamlessly integrate with each other
- Control communication between Worx-enabled apps
- Disable iCloud backup
- Allow WorxMail to open attachments in any Worx-enabled app
- Enable WorxWeb to open files and mailto links in any Worx-enabled app

Worx App SDK with MDX for application integration

MDX ensures that all Worx-enabled apps can interact with each other for a seamless experience. For example, clicking a link in WorxMail on an iOS device automatically opens WorxWeb, not Safari. A Microsoft® Word document from ShareFile can be opened with a published app from Citrix XenApp® while online and with a locally installed native mobile application when offline. This is done by offering only applications secured with XenMobile in the "Open with…" dialog that pops up when a user clicks on a Word document. In all cases the application and its data will be executed inside the secure container on the mobile device. No application residing outside the MDX container will be able to access the data. With WorxMail secured by MDX, users can attach docs to emails and save attachments using ShareFile, open attachments and send calendar invites using the free/busy information of attendees provided by WorxMail, all inside the secure container on the mobile device.

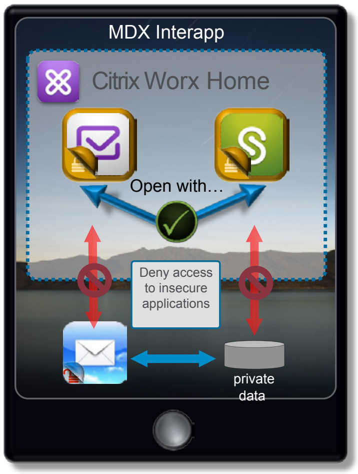


Figure 4. MDX allows work-enabled apps to communicate.

WorxMail supports Microsoft® ActiveSync® and Microsoft® Exchange and offers security features such as encryption for email, attachments and web links, including internal sites, WorxWeb enables simple, secure access to internal corporate web, external SaaS, and HTML5 web applications. WorxWeb leverages MDX Technologies such as the micro VPN to create a dedicated VPN tunnel for accessing a company's internal network and encryption for the browser cache, bookmarks, cookies and history.

In addition, MDX controls the communications between apps so that IT can enforce policies related to activities such as cut-and-paste between apps; for example, allowing cut-and-paste between Worx-enabled apps but not apps unprotected by the Worx App SDK, or by preventing use of a camera when using a specific Worx-enabled app.

Conclusion

XenMobile with the Worx App SDK (which includes MDX technologies) gives IT the power to separate business and personal applications inside a secure mobile container. In this container, employees are free to be productive while on the go. More importantly, the container prevents security from being compromised. MDX Technologies provide granular, policy-based management and access controls over all native and HTML5 mobile apps. IT can centrally control and configure policies based on users' identity, device, location and connectivity type to restrict malicious usage of corporate content. In the event a device is lost or stolen, business applications and data can be disabled, locked or wiped remotely. The overall result is a solution that increases employee satisfaction and productivity, while ensuring security and IT control.

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

About Citrix
Citrix (NASDAQ:CTXS) is the cloud company that enables mobile workstyles—empowering people to work and collaborate from anywhere, easily and securely. With market-leading solutions for mobility, desktop virtualization, cloud networking, cloud platforms, collaboration and data sharing, Citrix helps organizations achieve the speed and agility necessary to succeed in a mobile and dynamic world. Citrix products are in use at more than 260,000 organizations and by over 100 million users globally. Annual revenue in 2012 was $2.59 billion. Learn more at www.citrix.com.