Augmenting security and management of Office 365 with Citrix Endpoint Management (formerly XenMobile)

There are quite a few reasons why Microsoft Office 365 is so popular with enterprise customers.
Microsoft Office 365 allows organizations to move costly on-premises infrastructure including Microsoft Exchange, Lync and SharePoint into Microsoft’s cloud and still provide their users with the access they need. Add the popularity of traditional Office apps like Word, Excel and PowerPoint among users of tablets and smartphones and Microsoft’s server infrastructure in the cloud, and it is no wonder why securing and managing these apps is a common requirement.

In addition to Office 365 apps, most enterprise organizations deploy a vast array of other native mobile apps, as well as custom-built apps, web and SaaS apps, and even virtualized apps that run securely in the datacenter. IT requires visibility into all supported platforms and the apps and data they contain. Another requirement is some level of protection for corporate apps, and perhaps even isolation from personal apps, on users’ mobile devices. Lastly, IT needs the ability to selectively wipe corporate apps and data from mobile devices, should the need arise, without impacting the user’s personal presence on the device.

Referencing functionality in XenMobile, this paper discusses securely deploying and managing Office 365, protecting data at rest on a mobile device and protecting data in transit. It also explains how to configure XenMobile apps with hosted Exchange. XenMobile apps, which are enterprise-class apps from Citrix and its development partners, can help users gain additional productivity when using Office 365 hosted services and other Microsoft cloud products such as Azure Active Directory and Azure Rights Management Services.

Deploying Office 365 with XenMobile

Deploying Office apps to mobile devices is often the first step taken by IT after adopting Office 365. Some apps may be required for specific users, prompting IT to “push” them to the devices immediately upon enrollment. Other apps are optional, so IT wants to offer them to users via an enterprise app store. Office 365 productivity apps, including Word, Excel and PowerPoint, are offered by public app stores such as the Apple App Store, Google Play and Microsoft Marketplace.

Securing distribution to mobile users is very simple with XenMobile.

XenMobile empowers IT to:
- Securely deliver Office 365 and other mobile apps to authorized and compliant mobile devices
- Enforce policies regarding device encryption that protects data at rest
- Enable micro-VPN or per-app VPN protection of data in transit between the cloud and the internal enterprise datacenter or network

Specifically, when used with Office 365 services and apps, XenMobile allows IT to:
- Authorize the user, check the mobile device for compliance and deploy apps securely.
- Deploy Office 365 and other Microsoft native apps to devices through the single XenMobile enterprise app store.
- Configure the device’s native email and personal information manager (PIM) apps connecting to on-premises or Microsoft cloud-hosted services.
- Optionally deploy and configure XenMobile apps for Exchange and other Office 365

XenMobile and Azure Active Directory work together to deliver the centralized authentication that IT requires with the experience end-users need to remain productive.
hosted services to provide even better security and productivity.
• Store MAM apps in a secure MDX container protected by XenMobile (MDM apps rely on the mobile OS).
• Enforce device operating system containerization features like data separation, cloud backup restrictions, "open in" restrictions and selective removal of apps and data if the need arises.
• Protect Office 365 data while in transit to on-premises or Microsoft cloud-hosted services.
• Create a secure, per-app VPN tunnel to the on-premises service or cloud through NetScaler Gateway.
• Utilize geo-location and specific named network policies to enforce policies governing access services, thereby preventing devices from accessing non-authorized networks.

Following are details for each of these deployment steps.

**Securely deliver Microsoft Office 365 apps to mobile devices**

With XenMobile, deploying Office 365 apps to mobile users is quite simple. The XenMobile enterprise app store is contained within the Secure Hub (enrollment) app. The XenMobile Store can contain any app that the organization wishes to make available to its users, including:
• Enterprise apps designed and built by the organization’s development environment or acquired from third parties.
• MDX apps and apps that can be wrapped by the organization using the MDX Service (for cloud and hybrid deployments), the MDX toolkit (for on-prem deployments), the Secure App SDK, or apps acquired from third parties and wrapped.
• Public app store apps from the Apple iTunes Store, Google Play, etc.
• Web-based and SaaS apps located on the internal network or delivered over a public network, including apps that utilize single sign-on (SSO) authentication.
• Web links - web addresses (URLs) of public or private sites, that do not require SSO.

This paper focuses on adding Microsoft Office 365 public apps to the XenMobile Store. Users can easily access the Store immediately following enrollment of their device in the XenMobile environment. The list of apps shown to each user is based on user name (Active Directory or other group membership) and the device parameters (type, platform, size, etc). These lists, as well as the policies and rules that apply to each app and the approval workflow for specific users, are defined by IT. As a user moves to a different group (such as a transfer from sales to marketing) due to a new job role or IT decision, he or she will automatically be assigned new apps, policies, and approval workflows.

Mobile devices should be compliant before access to enterprise apps is granted. XenMobile provides a complete compliance check during the initial enrollment process using Secure Hub. This process ensures only authorized devices can access published enterprise apps.

**The XenMobile model for distributing apps**

The Store is contained within the Secure Hub native app, which also provides enrollment, compliance and SSO services. Users download Secure Hub from public app stores such as iTunes App Store or Google Play.
IT can easily build “delivery groups within the XenMobile administration console. These deployment packages can be a combination of policies, apps and approval workflows assigned to Active Directory or other user groups. Assignment to groups makes the administration experience very scalable.

Apps can be configured as “required” or “optional.” Required apps are pushed to the device immediately upon enrollment. Optional apps can be viewed and downloaded from the Store after enrollment.

If employees plan to use the native email and PIM apps on their devices, XenMobile can easily configure those apps to connect to email servers either located on premises or hosted in the cloud, such as Microsoft Office 365 Exchange servers.

Using XenMobile to distribute Office 365 apps

Deploying Office 365 apps (Word, Excel, PowerPoint) follows exactly the same procedure as deploying any other app. IT can easily search public app stores using the app name or partial name to display a list (Figure 3). Unlike other enterprise mobility management (EMM) products, XenMobile does not require IT to look up the confusing AppID (for example, com.microsoft.Office.Word).

Once the app has been found (Figure 4), IT can configure how it will be displayed in the Store. The name and description of the app are automatically pulled from the public app store, but they can be modified by IT if desired.

Other options include a customized FAQ to educate users on the app, customized screen shots and the opportunity to let users provide reviews and ratings of the app (Figure 5). These features are especially valuable for custom enterprise apps, but can also be used for apps from public stores to create a friendlier, consumer-like experience for the enterprise app store.

IT can set additional options, like the ability to use the Apple “managed app” API to force the app to be deleted if the user un-enrolls in XenMobile. Another option is configuring the app not to backup data with the Apple iCloud service.

Protect data at rest on the device

The mobile application management (MAM) capabilities in XenMobile enable complete...
Figure 3: Search public app stores

Figure 4: Configure how it will be displayed in the Store

Figure 5: Options include customized FAQ, screenshots or app reviews and ratings
Citrix XenMobile MAM

MDX app 1

Open-In
MDX Policies

Interception Layer

mobile OS

MDX app 2

Microsoft Intune MAM

XenMobile Secure Mail

Open-In
MDX Policies

Interception Layer

mobile OS

Figure 6: XenMobile allows for seamless Open-In functionality between Secure Mail and O365 apps

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

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

Citrix XenMobile allows for seamless Open-In functionality, so users can exchange data and documents with native Office apps. For example, an attachment in XenMobile Secure Mail can seamlessly be opened in various Microsoft Office 365 apps.

Beyond device and application policy control, the best way to safeguard data at rest is encryption (Figure 6). While most EMM vendors simply enable the device’s default encryption mechanism, Citrix has taken an extra step by providing an additional layer of encryption for any data stored in a XenMobile-enabled app. The MDX App SDK utilizes FIPS 140-2-compliant AES 256-bit encryption with keys stored in a protected Citrix Secret Vault.

In addition, XenMobile includes platform and device specific technologies like Samsung Knox, Google Android for Work and Apple Managed Apps.

XenMobile also supports Windows 10, as well as Windows Information Protection (WIP) providing control over “open in” and copy/paste actions.

Secure data at rest within Microsoft Office 365 apps

Enabling and enforcing the device’s built-in encryption is critical. IT can use XenMobile to configure and enforce device-native OS containerization controls to help secure data at rest within Office 365 apps.

When deploying Office 365 apps through the XenMobile Store, IT can configure the appropriate security policies and selectively wipe the apps and their data from the device if needed.

How to secure Office 365 apps on Android devices with Android for Work

• XenMobile can configure the native email and PIM apps in the Android for Work container to connect to the Office 365 hosted Exchange service.
• XenMobile can configure and manage the Android for Work container, which will contain the Office email, PIM and other business apps, allowing IT to set appropriate DLP policies such as screen capture and copy/paste restrictions.
• XenMobile can selectively wipe the Android for Work container, including all of the organization’s apps and their data, from the device if the need arises.
• If the device goes out of compliance with any of IT’s policies, the Android for Work container can be temporarily locked until the user returns the device to a compliant state.
• If IT chooses to deploy Secure Mail instead of using the device’s native email client, additional DLP policies pertaining to email and attachments and located in on-premises Active Directory or in Azure (Active Directory Microsoft Rights Management Services) will be honored.

How to secure Office 365 apps on iOS devices

XenMobile can configure the native email and PIM apps on the iOS device to connect to the Office 365 hosted Exchange service.

• XenMobile can configure the email/PIM accounts as managed accounts (keeping the
user from moving mail from the business account into a personal account) and all of the Office apps as managed apps (allowing for selective removal).

- XenMobile can enforce additional DLP control over other business apps and email accounts.
- XenMobile can selectively wipe all Office 365 apps, Office 365 email accounts and data from the device should the need arise (employee departure, contract expiration, lost, stolen or noncompliant device).
- XenMobile can configure the device to utilize the Citrix VPN to securely tunnel all network connections to Office 365 through NetScaler Gateway.
- If IT chooses to deploy Secure Mail instead of using the device’s native email client, additional DLP policies pertaining to email and attachments and located in on-premises Active Directory or in Azure (Active Directory Microsoft Rights Management Services) will be honored.

Protecting data in transit

Unauthorized or unsecure network connectivity can be a major threat vector for mobile devices. Today’s devices are very powerful. They support an expanding array of connection features, such as acting as a mobile hotspot. If left on and unsecured, this capability could allow unauthorized connectivity and potentially leak data.

IT needs to protect the connection from the mobile device to corporate services like ActiveSync. XenMobile can help IT filter out unwanted connections to this critical service and allow only authorized devices and clients. For example, XenMobile can be configured to block all ActiveSync connections unless the device/client is enrolled and managed.

XenMobile Mail Manager integrates directly with Exchange and Office 365 hosted Exchange using the PowerShell management client to enable/disable ActiveSync for specific users. For example:

- ActiveSync is disabled (from Active Directory policy) for all users.
- Users enroll their device in XenMobile.
- XenMobile connects to on-premises Exchange or cloud-hosted Office 365 Exchange to issue a command enabling ActiveSync on that user’s account and device.
- If a compliance rule is broken, XenMobile can disable that device’s connection to ActiveSync.

Some customers have “private” connections to their Office 365 instance and do not allow Internet connectivity. Using the Citrix VPN client through NetScaler Gateway allows the mobile device to connect to Office 365 through the existing secure corporate connection. NetScaler Gateway, a FIPS-compliant gateway, allows the organization to maintain end-to-end FIPS-compliant connectivity.

Additionally, NetScaler Gateway can be configured using “step-up security” to require a second authentication factor (like a secure token) to make the connection.

Using Office 365 hosted services with XenMobile apps

XenMobile apps like Secure Mail provide a more enterprise-like user experience than Microsoft Outlook. Leveraging features such as the ability to auto-join meetings or conference calls, schedule web and audio meetings or show an invitee’s calendar availability when scheduling a meeting, Secure Mail provides more business features than users are accustomed to from using Outlook on their desktop.

How to configure Secure Mail to use Office 365 hosted Exchange

Only two configuration settings matter when configuring Secure Notes, the secure note-taking app, to use the Office 365 version of Exchange.

1. Configure network connectivity (Set up the same as for Secure Mail shown in Figure 7) – A customer running an on-premises version of Exchange combined with the micro-VPN capabilities of NetScaler Gateway would normally want the connection to be tunneled through the micro-VPN to the Exchange server. To do this, set Network Access in the XenMobile console to Tunneled to the internal network, which will allow the app to create the secure micro-VPN to NetScaler Gateway and connect to the Office 365 service from that network. Alternatively, set this option to Unrestricted, which means the device will not use a secure tunneled connection, but instead will connect directly over the Internet to the Office 365 service.

2. Configure the email server (Figure 8) – Under the App Settings section, set the Secure Mail Exchange Server to outlook.office365.com.

How to configure Secure Notes to use Office 365 hosted Exchange

Only two configuration settings matter when configuring Secure Notes, the secure note-taking app, to use the Office 365 version of Exchange.

1. Configure network connectivity (Set up the same as for Secure Mail shown in Figure 7) – A customer running an on-premises version of Exchange combined with the micro-VPN capabilities of NetScaler Gateway would normally want the connection to be tunneled through the micro-VPN to the Exchange server. To do this, set Network Access in the XenMobile console to Tunneled to the internal network, which will allow the app to create the secure micro-VPN to NetScaler Gateway and connect to the Office 365 service from that network. Alternatively, set this option to Unrestricted, which means the device will not use a secure tunneled connection, but instead will connect directly over the Internet to the Office 365 service.

2. Configure the email server – Under the App Settings section, set the Secure Notes Exchange Server to outlook.office365.com

Optionally, with Secure Notes IT can control the version that users choose. Secure Notes “+” uses the employee’s ShareFile storage for synchronizing data. This version provides much richer note-taking experience for enterprise scenarios (the ability to add photos, videos and audio and metadata like tags) but does not synchronize notes taken in Outlook and saved to Exchange. However, you may still wish to configure the Exchange server entry because Secure Notes will use this information to synchronize the user’s calendar information so that notes can be linked to meetings and easily shared with all invitees. Alternatively, Secure Notes provides the basic Exchange note-taking experience and will
Figure 7: Configure network connectivity for Secure Mail to use Office 365 hosted exchange

Figure 8: Configure email server for Secure Mail to use Office 365 hosted exchange

Figure 9: Configure network connectivity for Secure Notes to use Office 365 hosted exchange
synchronize with Exchange notes.

**How to configure Secure Tasks to use Office 365 hosted Exchange**

Two configuration settings are important when configuring Secure Tasks, the enterprise mobile app that allows users to manage their tasks from Microsoft Outlook, to use the Office 365 version of Exchange.

1. **Configure network connectivity (Set up the same as for Secure Mail shown in Figure 10)**
   - A customer running an on-premises version of Exchange combined with the micro-VPN capabilities of NetScaler Gateway would normally want the connection to be tunneled through the micro-VPN to the Exchange server. To do this, set **Network Access** in the XenMobile console to **Tunneled to the internal network**, which will allow the app to create the secure micro-VPN to NetScaler Gateway and connect to the Office 365 service from that network. Alternatively, set this option to **Unrestricted**, which means the device will not use a secure tunneled connection, but instead will connect directly over the Internet to the Office 365 service.

2. **Configure the email server** — Under the **App Settings** section, set the Secure Tasks Exchange Server to **outlook.office365.com**.

**How to configure Secure Mail to allow email attachments to “open in” Office apps**

Normally, the MDX-enabled version of Secure Mail will be configured to restrict data export (moving files from one app to another app), but in some cases, you may wish to allow an exception to this policy. A good example would be to allow Microsoft Office documents (attachments) to be opened in the Office apps installed on the device.

XenMobile allows you to configure a normally restricted data exchange policy (deny “open in” non-MDX-enabled apps), but provide an exception list of apps that are allowed (deny “open in” non-MDX apps PLUS these excluded apps). (Figure 11)
To configure the policy in XenMobile:

1. Upload the MDX file as normal in the XenMobile UI.


Don’t forget to check your configurations with XenMobile Analyzer

Citrix XenMobile Analyzer is a free, one-stop, cloud service for diagnosing any XenMobile-related issues, whether it’s an on-prem or cloud deployment. Any XenMobile administrator that has a MyCitrix account can use it to access any of the five tests the Analyzer provides.

The tests included are the XenMobile Environment test, the NetScaler Configuration test, the Secure Mail test, which helps with sorting out ActiveSync issues, Server Connectivity tools which advise on configuring your servers and Citrix Insight Services which provides information about your infrastructure.

Conclusion

Use EMS/Intune MAM to manage O365 apps plus XenMobile to enhance O365 security and everything else.

Microsoft Office 365 hosted services and Office productivity apps provide a great work environment for mobile users, and undoubtedly will play an increasing role in any enterprise’s mobility strategy. Using XenMobile from Citrix, IT can centrally control and configure policies based on user 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 using XenMobile MDM capabilities. The enterprise grade and scale offered by XenMobile and NetScaler Gateway are unparalleled in the industry for securing and managing Microsoft Office 365 apps and data. The overall result is a solution that increases employee satisfaction and productivity, while ensuring security and IT control.

By using XenMobile Analyzer, 40% of XenMobile customers were able to solve issues without contacting Citrix.