XenApp, XenDesktop and XenMobile Integration

for a Comprehensive Mobility and Digital Workspace Solution
Desktop and application virtualization have enhanced mobility everywhere, allowing users to access their Windows desktops and applications securely from any location on any device at any time, whether in patient rooms, on the road or in the field. Application and desktop virtualization via Citrix XenApp and XenDesktop are essential components of mobility strategies in thousands of security-sensitive organizations, enabling IT to store virtualized Windows endpoints in a centralized datacenter or the cloud so they can be easily secured and managed at all times.

Today, however, virtualization is just a single component of a fully mobile digital workspace experience. Corporate Owned, Personally Enabled (COPE) and Bring Your Own Device (BYOD) initiatives have merged personal and work worlds on millions of mobile devices including smartphones and tablets. While desktop virtualization can enable Windows to work on these devices securely, some employees have demanded the use of native mobile apps, in some instances in combination with virtual Windows desktop apps. While desktop virtualization can enable Windows to work on these devices securely, some employees have demanded the use of native mobile apps, in some instances in combination with virtual Windows desktop apps. In addition, some employees prefer to use their own device mixing work-related mobile apps with their personal mobile lifestyles on a single device. At first, it’s about email access and file sharing using native mobile apps, but eventually employees and their organizations expect mobile applications that facilitate organizational workflows and other important work functions. For a complete digital workspace, employees need access to any app from any device.

In this environment, IT must not only discover, inventory and manage all employee connected mobile devices across their lifecycle, but protect enterprise information and mobile applications from the devices’ personal counterparts, which, unmanaged, increase the risk of enterprise malware infection and data breaches. In addition, if any data is stored on the mobile device, IT needs to ensure that the data is encrypted.

That’s why enterprises have invested heavily in enterprise mobility management (EMM) and Unified Endpoint Management (UEM) solutions that combine mobile device management (MDM) with mobile application management (MAM) and security, empowering COPE and BYOD programs with minimal risk. The good news for Citrix users: Not only is Citrix the market leader in desktop and application virtualization solutions with XenApp and XenDesktop, it also offers a full-featured XenMobile Enterprise Mobility Management and Unified Endpoint Management solution that integrates tightly with XenApp and XenDesktop. XenMobile users get full access to all their mobile, Windows, web, and SaaS cloud applications from a single unified storefront and a single storage solution for their confidential files. IT gets tight integration across EMM and desktop virtualization, and a single vendor for support and licensing. Here’s how current XenApp and XenDesktop enabled enterprises can adopt Citrix XenMobile and integrate it tightly with XenApp/XenDesktop to deliver this full solution to the mobile user.

**XenMobile EMM and UEM**

Citrix XenMobile is a full-featured enterprise mobility management solution that allows IT to discover, secure, apply policies to, and manage all of its users’ smart phones, tablets, and laptops running iOS, Mac OS, Windows, and Android. Not only does XenMobile provide comprehensive classic mobile device management (MDM) capabilities, such as device discovery, lifecycle management, policy enforcement, user self-enrollment, and remote device lock and wipe, it also includes full application wrapping, containerization, an enterprise app store, and data security features that allow users to mix enterprise applications and data with their personal applications and data safely, without risk of enterprise malware infections or data breaches.

XenMobile also empowers users with secure mobile productivity apps including enterprise class email and Web browsing. Both XenMobile Enterprise Edition and the new XenMobile Premium Service also include ShareFile, a secure, enterprise-class file sharing and collaboration alternative to consumer file sharing solutions such as DropBox and Box, providing users secure access to all their files on any device. Once XenMobile and XenApp or XenDesktop are integrated, users will be able to access their XenApp and XenDesktop
apps and thus their Windows desktops within Secure Hub (fka: Worx Home) as well, without having to log in separately. With Citrix XenMobile users can combine corporate and personal lifestyles easily, without burdensome restrictions, while corporate IT can track and secure all the mobile devices, applications and information of its users.

Example Customer Use Case

A large international bank envisioned a more mobile workforce. Plans were already in place to deploy a previous investment in desktop virtualization (based on XenApp and XenDesktop), increasing flexibility within the bank’s call centers, and the bank had already issued smartphones and tablet devices to a small number of employees (where remote access was deemed essential). In reality, many more employees were accessing corporate information from personal devices. The IT team was keen to help more employees improve their personal productivity by creating a more mobile workspace, but maintaining the security of sensitive corporate information was of critical importance.

The team then determined that any enterprise mobility solution had to allow users to securely access data and applications from anywhere, on personal as well as company-owned devices. More importantly, it also had to allow email attachments to be saved locally and edited on the device. In addition, the team determined that any enterprise mobility solution had to work seamlessly with all existing infrastructure and be resilient on sub-standard networks that often included lines running at just 128kbps or even 64kbps.

The team decided to integrate XenMobile as the company already had a large Citrix infrastructure and XenMobile met all the requirements of a complete Enterprise Mobility Management solution.

After integrating XenMobile into their environment, XenMobile has not only secured the bank’s business information used by remote workers across Africa, it has also provided a much improved user experience. Bank staff can now securely access email, intranet sites and a range of centrally managed line-of-business applications on any device (bank-owned or personal), even on sub-standard connections — improving their productivity. At the same time, should a device ever be lost or stolen, access to sensitive resources can be withdrawn instantly. The addition of ShareFile (which has become the bank’s approved document sharing solution for mobile workers), has created a platform for effective mobile working.

Citrix Cloud integration of XenApp, XenDesktop, XenMobile, ShareFile and NetScaler

In most organizations, the Citrix XenApp and XenDesktop architecture consists of a XenApp or XenDesktop server farm fronted by Citrix StoreFront, which provides access to the users’ Windows applications, and a NetScaler Gateway, which provides an SSL VPN gateway, application load balancing, and access control. Desktop and laptop clients run Citrix Receiver client software to connect to their Windows apps and desktops remotely. Once XenMobile is installed and configured, it typically sits behind the NetScaler in the DMZ. XenMobile also includes an enterprise
app store, which provides mobile users with access to approved mobile, Windows, web, and SaaS applications based on user groups and rights configured in Microsoft Active Directory.

Integration comes through StoreFront Server, where information can be pulled from XenApp and XenDesktop and added into the enterprise app store through XenMobile. This provides mobile users with their Windows applications or full Windows desktop, along with all their other mobile, web, and SaaS applications, from a single pane of glass.

**Step-by-Step Instructions**

Here are the steps you need to follow to integrate XenMobile with XenApp and XenDesktop so that users can access their Windows desktops and applications directly from Secure Hub.

1. **Add a Secure Ticket Authority (STA) for the XenApp/XenDesktop Controllers to the XenMobile NetScaler Gateway**

   This is an essential step that can easily be forgotten, but is absolutely essential for providing users with secure, controlled access to their Windows applications and information. Open the NetScaler console, open the Gateway vServer used for XenMobile in NetScaler, which in XenMobile 10.5 has a default name of _XM_XenMobileGateway. Go to the STA (Secure Ticket Authority) Server Bindings and make sure the XenApp and/or XenDesktop controllers and the XenMobile server are added.

2. **Add the XenMobile NetScaler Gateway to the Remote Access Settings on the StoreFront Server**

   This enables the XenApp/XenDesktop StoreFront Server to talk with the XenMobile NetScaler Gateway. Open the StoreFront Console, go to Stores, and click Enable Remote Access on the left side of the screen.

   Click Add and fill in the required information about the XenMobile Gateway vServer, including URL, version, subnet if relevant, logon type and callback URL.
Click Next and add the XenApp or XenDesktop Controllers as STA’s. These must be the same as the STA’s configured in the XenMobile Gateway vServer in NetScaler.

Click Create to get to the Enable Remote Access Screen and make sure both the StoreFront and XenMobile Gateway are selected. Then click OK.

3. Enable XenApp Services Support on the StoreFront Server

On the next screen, click the box next to Configure XenApp Services Support and specify a default store for the users. Copy the XenApp Service URL displayed to a notepad as you’ll need this path later when enabling XenApp or XenDesktop integration within XenMobile.

4. Add the StoreFront Host Information into the XenMobile Server

This ensures the XenMobile Server can connect to the StoreFront Server. Make sure all the certificates necessary for XenMobile to communicate with StoreFront using SSL are loaded. Open the XenMobile console and log in as an Administrator.

Open the Configure tab, go to the Settings page and click on XenApp and/or XenDesktop. Then fill in the relevant Host, Port, and relative path, the latter of which is the URL you copied in the previous step. If you are using HTTPS for your StoreFront, enable it. Then click Save.

5. Deploy Citrix Receiver to the Mobile Devices

If you are using Secure Hub 10.3 or newer, there is no need to install Citrix Receiver on the mobile device. If you are using Secure Hub 10.2 or earlier, you can use XenMobile to push Citrix Receiver to all mobile devices. Receiver doesn’t have to be configured in any way on each device, just present.

Assuming all the steps were followed, you’re done on the back end. Users can open Secure Hub on any connected device and access the Enterprise App Store. They will see their Windows apps and Desktops listed alongside their mobile, web, and SaaS apps. They can now click on them to add them to their device. When they launch the apps, there is no need for a second authentication for XenApp/ XenDesktop since they have already authenticated to Secure Hub.

By integrating XenApp and XenDesktop with XenMobile, you provide your mobile users with all of their mobile apps, Windows apps and desktops, SaaS, and web applications from a single sign on and interface on any device. The result is a full mobile workspace solution at the lowest possible cost and risk to your organization.

For more information, speak to your Citrix sales representative. In addition, current XenApp and XenDesktop customers should inquire about the Citrix Workspace Suite Trade-up Program which provides promotional discounts to XenMobile.