Managing Windows 8.1 Devices with XenMobile

Mobile Device Management for Windows 8.1 Devices

The “Bring Your Own Device” Challenge

With the advent of the “bring your own device” (BYOD) trend, employees expect to bring their personal mobile devices to work, and to use these devices on the corporate network for their work tasks. This poses new challenges for a company’s IT team—these employee-owned personal devices must be managed and secured, as they will access corporate applications and sensitive corporate data. How do you block access to corporate applications, resources and data when the employee leaves the company, or if their device is stolen? How do you enforce security settings and passcodes on their personal devices so that sensitive corporate data isn’t compromised if the device is lost or stolen?

Over the last five years, Mobile Device Management (MDM) solutions that address the challenges of managing both corporate and employee-owned devices have matured. These solutions now provide sophisticated device management capabilities, including the enforcement of passcodes, device provisioning, limiting access to corporate applications and resources based on an employee’s job role, and wiping all corporate applications and data from a device when an employee leaves the company or their device is lost or stolen.

Specific Windows 8.1 MDM Challenges

Until recently, most MDM products focused primarily on managing iOS and Android devices, as those mobile operating systems include application programming interfaces (API) with management “hooks” into the devices. As Microsoft Windows 8.1 devices such as Surface tablets became available and employees began bringing them to work, a problem arose. Windows 8.1 did not initially include open MDM APIs to enable third party MDM solutions to adequately manage Windows 8.1 devices. As a result, companies that invested in an MDM solution to manage their iOS and Android devices were typically forced to use a separate Microsoft solution to manage Windows 8.1 devices, increasing the company’s device management efforts and associated costs.

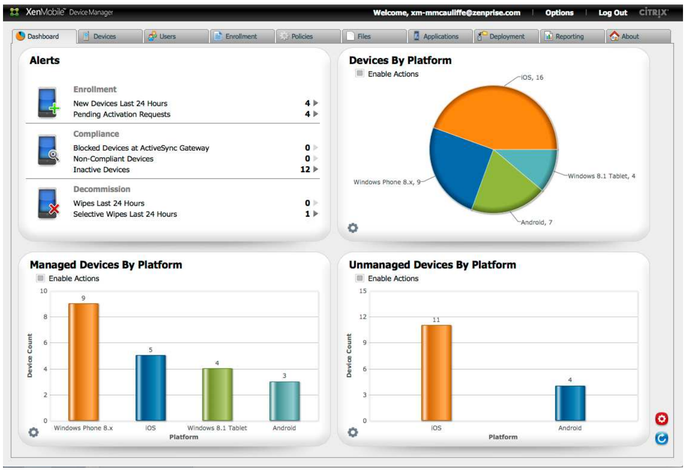
However, with the recent addition of open MDM APIs to Windows 8.1, companies can now manage a heterogeneous mix of iOS, Android and Windows 8.1 mobile devices from a single MDM solution. For example, Citrix’s XenMobile MDM solution leverages these new Windows 8.1 MDM APIs, enabling companies to manage all employee mobile devices—both corporate and employee-owned, and all device types—from a single MDM solution. XenMobile 8.7 included initial support for Windows 8.1 device management, including Surface tablets and laptops. The latest release, XenMobile 9.0, takes this support even further, adding more comprehensive management capabilities for Windows 8.1 devices.

This paper demonstrates how to enroll a Windows 8.1 device with a XenMobile MDM server. It also includes an overview of the specific security policies and management options available for Windows 8.1 devices once they are enrolled with XenMobile.

XenMobile and Windows 8.1

XenMobile easily configures Windows 8.1 devices with, among other things, security policies, credentials, device restrictions, password policies, VPN and WiFi settings, and web clips. XenMobile also collects a hardware inventory from enrolled Windows 8.1 devices and can send commands to lock or selectively wipe (remove all corporate data and settings) Windows 8.1 devices if lost or stolen.

The screenshot below shows the XenMobile web-based administration console's **"Dashboard"** tab. This tab provides a quick overview of the number and types of devices enrolled with and managed by the XenMobile MDM server. Alerts are also displayed for devices that were recently enrolled, are non-compliant with corporate security policies, or have recently been wiped or selectively wiped.



Alerts

Enrollment

New Devices Last 24 Hours	4
Pending Activation Requests	4

Compliance

Blocked Devices at ActiveSync Gateway	0
Non-Compliant Devices	0
Inactive Devices	12

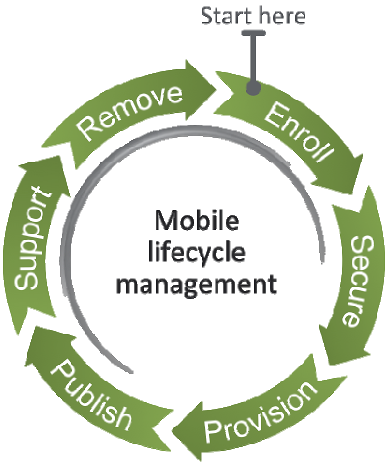
Decommission

Wipes Last 24 Hours	0
Selective Wipes Last 24 Hours	1

Administrators and security personnel use this administration console to quickly and easily define security policies and device configuration settings to be pushed to Windows 8.1 devices when they enroll, and for ongoing device monitoring and management.

Mobile Device Management Lifecycle

The diagram below shows the typical management lifecycle of a Windows 8.1 device in a corporate environment.



First, when an employee begins to use their mobile device on the company network, they enroll the device with the corporate XenMobile Mobile server. For Windows 8.1 devices the agent used to enroll the device with the server is part of the Windows 8.1 operating system, and the user doesn't have to install a separate MDM agent application before the device can be enrolled.

After the device is enrolled (shown later with a series of screen shots) by entering corporate Active Directory credentials and following several prompts, XenMobile secures and provisions the device for use on the company network.

XenMobile rapidly provisions the device for the user's corporate access and needs. Network configuration settings (VPN, WiFi, etc.) are pushed to the device at enrollment time, eliminating the typical series of phone calls to the IT help desk or colleagues to figure out how to get a new device onto the network. XenMobile automates the entire process, greatly speeding up and improving the end user experience.

To enhance security, an MDM policy can require the device owner to set a password, and other device restrictions can be pushed to the device during enrollment.

Ongoing support is also a key requirement. If a user loses their device, or it is stolen, an administrator can send a Lock or Selective Wipe command to the device via XenMobile's administration console. This ensures that device access to the corporate network is disabled, and that all corporate data and applications are removed from the device.

Finally, XenMobile can detect when a user is disabled in Active Directory, for instance when they leave the company, and then use "automated actions" to automatically send a Selective Wipe command to all of the user's devices. This eliminates the need for manual action by an administrator and the possibility of this important activity falling through the cracks.

Setting Up Auto-discovery for Device Enrollment

The screen shots and descriptions in the next section show how to enroll a Windows 8.1 device with XenMobile. A Surface RT 8.1 tablet is enrolled with a XenMobile MDM server. Note that the user account on the Windows 8.1 device must be a device Administrator's account in order to enroll the device.

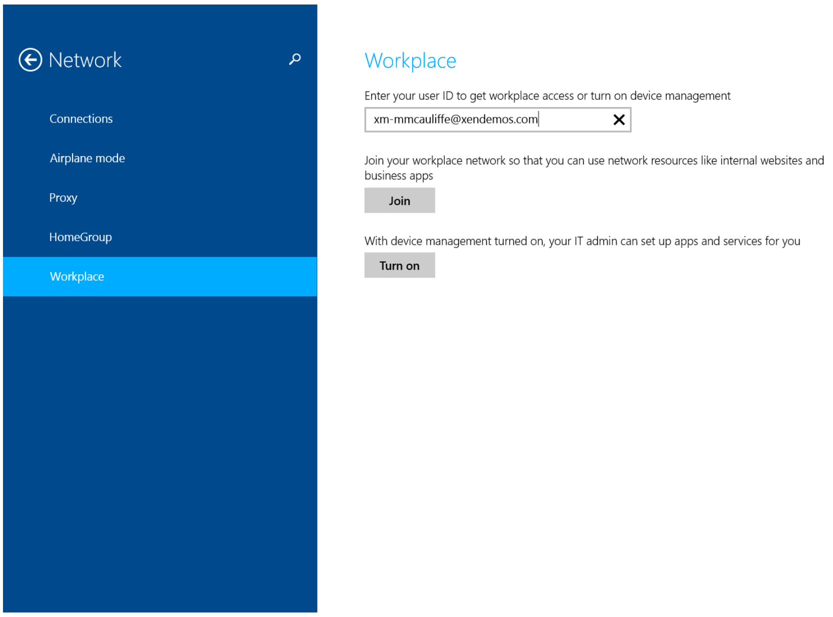
The XenMobile environment must also be registered with Citrix for "auto-discovery" of the XenMobile MDM server by enrolling devices. To do this you must provide Citrix with an SSL certificate for enterpriseenrollment.*mycompany*.*com*, where *mycompany*.*com* is the domain containing the accounts with which users will enroll. For more details, see the Citrix eDocs at:

http://support.citrix.com/proddocs/topic/xenmobile/xmob-landing-con.html

Setting up auto-discovery streamlines the enrollment process for users. They simply provide their Active Directory credentials (username/password) when enrolling a device, and don't need to know or enter the address of the corporate XenMobile MDM server.

Enrolling a Windows 8.1 Device with XenMobile

A user provides their AD user credentials (email address and password) to begin enrolling a Windows 8.1 device with XenMobile. They are then guided through the enrollment process. To do this, go to the **Network** settings screen and select the **Workplace** settings. Enter your user ID (email address) and select the **"Turn on"** button.



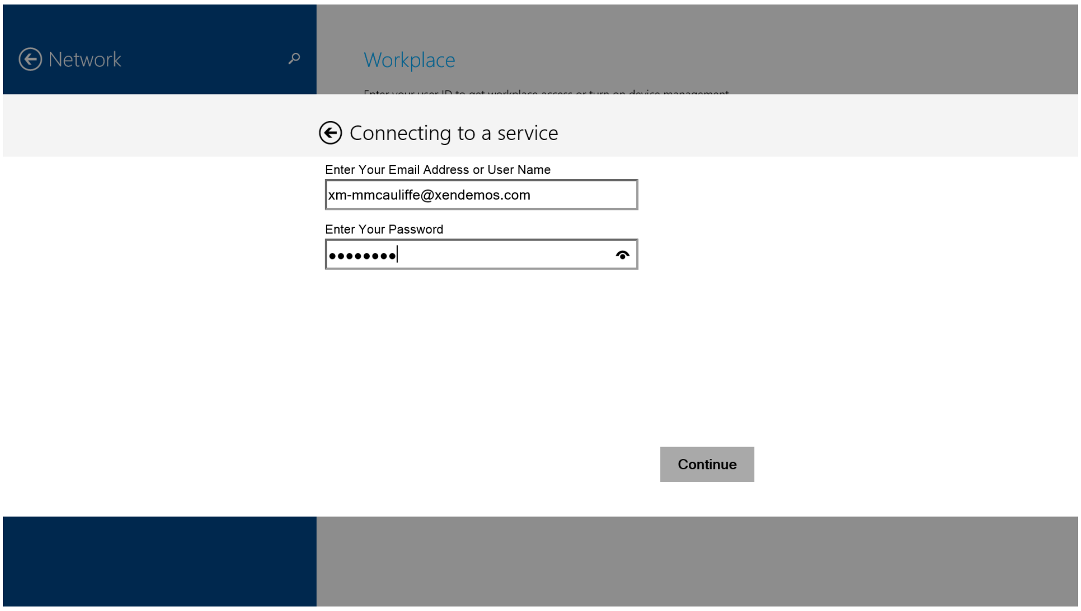
Enter your user ID to get workplace access or turn on device management

xm-mmcauliffe@xendemos.com

Join your workplace network so that you can use network resources like internal websites and business apps

With device management turned on, your IT admin can set up apps and services for you

Next, the **"Connecting to a service"** screen is displayed. Enter your Email Address again and your Active Directory Password. Select **"Continue"**



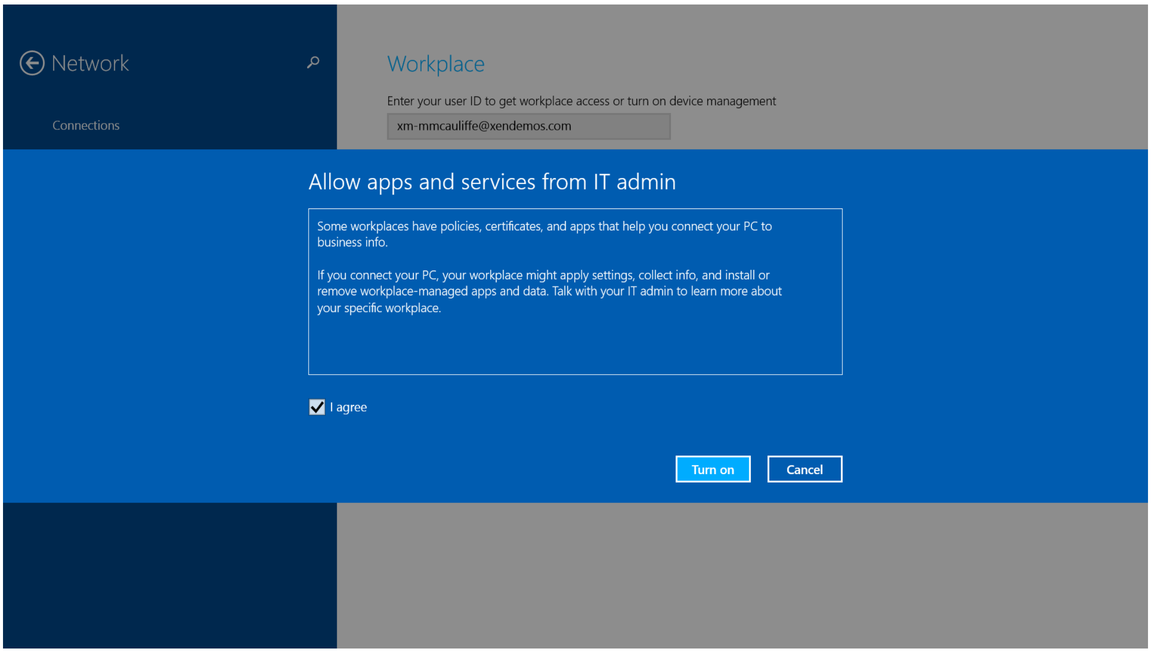
Enter Your Email Address or User Name

xm-mmcauliffe@xendemos.com

Enter Your Password

••••••••

Next, a terms and conditions screen is displayed to let you know that some features of your device are going to be managed by XenMobile. Check the **“I agree”** box and then click on the **“Turn on”** button.



Workplace

Enter your user ID to get workplace access or turn on device management

xm-mmcauliffe@xendemos.com

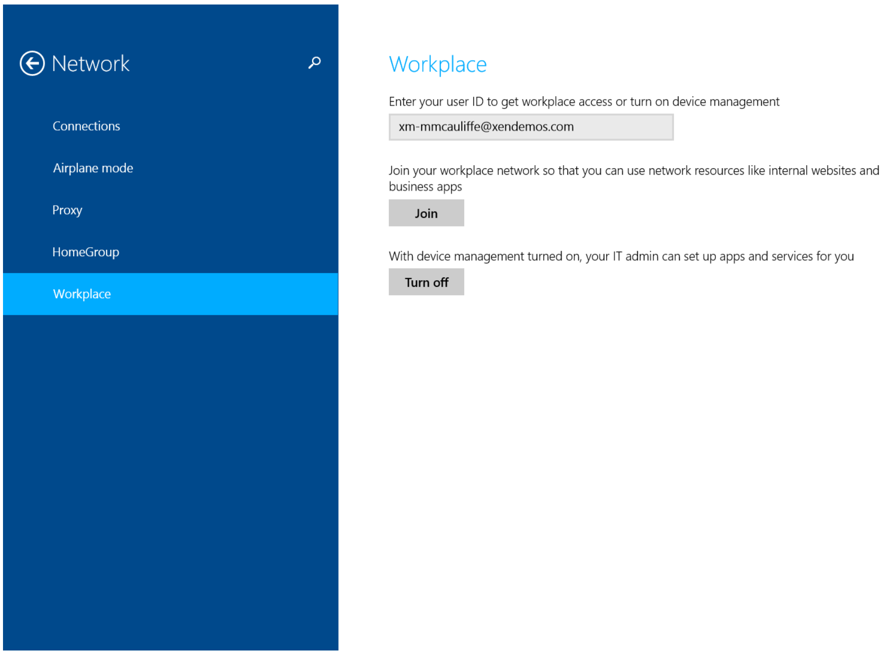
Allow apps and services from IT admin

Some workplaces have policies, certificates, and apps that help you connect your PC to business info.

If you connect your PC, your workplace might apply settings, collect info, and install or remove workplace-managed apps and data. Talk with your IT admin to learn more about your specific workplace.

☑ I agree

Device enrollment with XenMobile is now complete. To un-enroll the device at a future time, come back to the **Network** settings screen and click on the **“Turn off”** button.



Workplace

Enter your user ID to get workplace access or turn on device management

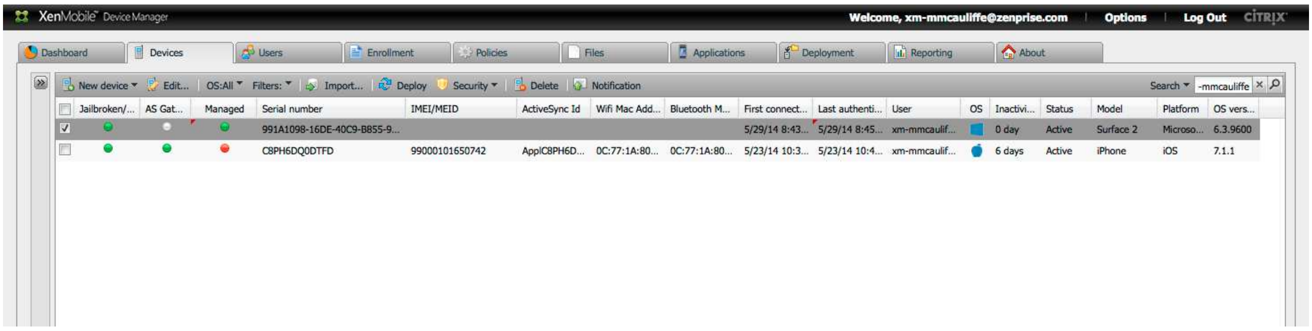
xm-mmcauliffe@xendemos.com

Join your workplace network so that you can use network resources like internal websites and business apps

With device management turned on, your IT admin can set up apps and services for you

Managing Windows 8.1 Devices with XenMobile

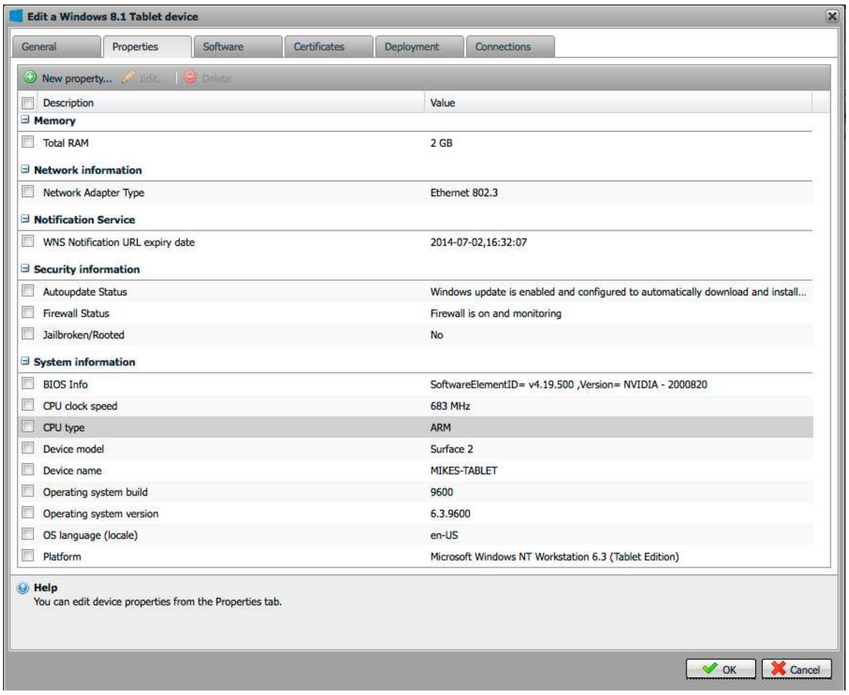
Administrators use the XenMobile web-based administration console, shown in the screenshot below, to define configuration policies and settings to be pushed to mobile devices at enrollment, and to monitor devices after enrollment.



☐	Jailbroken/...	AS Gat...	Managed	Serial number	IMEI/MEID	ActiveSync Id	Wifi Mac Add...	Bluetooth M...	First connect...	Last authenti...	User	OS	Inactivi...	Status	Model	Platform	OS vers...
☑	●	○	●	991A1098-16DE-40C9-B855-9...					5/29/14 8:43...	5/29/14 8:45...	xm-mmcaulif...		0 day	Active	Surface 2	Microso...	6.3.9600
☐	●	●	●	C8PH6DQ0DTFD	99000101650742	ApplC8PH6D...	0C:77:1A:80...	0C:77:1A:80...	5/23/14 10:3...	5/23/14 10:4...	xm-mmcaulif...		6 days	Active	iPhone	iOS	7.1.1

The **"Devices**" tab provides a list of all devices that have been enrolled with XenMobile. The top (highlighted) device in the list is a Microsoft Windows 8.1 Surface tablet that was just enrolled with XenMobile. (Other devices have been enrolled with the server—in this case the list has been filtered to show only devices owned by a specific user.) The Devices tab provides a quick look at the status of each enrolled device, including whether the device is still being managed, Jailbroken/Rooted status of the device, the device type, Platform, OS Version, etc.

Drill down on a device to learn even more about its detailed properties by selecting the device from the list and clicking on the "Edit" button. Click on the "Properties" tab of the window that is displayed, and a device hardware inventory is presented. This includes information about the device's memory, network hardware, security Information and additional "System information" such as operating system version, CPU type, clock speed, etc.



☐ Description	Value
⊟ **Memory**	
☐ Total RAM	2 GB
⊟ **Network information**	
☐ Network Adapter Type	Ethernet 802.3
⊟ **Notification Service**	
☐ WNS Notification URL expiry date	2014-07-02,16:32:07
⊟ **Security information**	
☐ Autoupdate Status	Windows update is enabled and configured to automatically download and install...
☐ Firewall Status	Firewall is on and monitoring
☐ Jailbroken/Rooted	No
⊟ **System information**	
☐ BIOS Info	SoftwareElementID= v4.19.500 ,Version= NVIDIA - 2000820
☐ CPU clock speed	683 MHz
☐ CPU type	ARM
☐ Device model	Surface 2
☐ Device name	MIKES-TABLET
☐ Operating system build	9600
☐ Operating system version	6.3.9600
☐ OS language (locale)	en-US
☐ Platform	Microsoft Windows NT Workstation 6.3 (Tablet Edition)

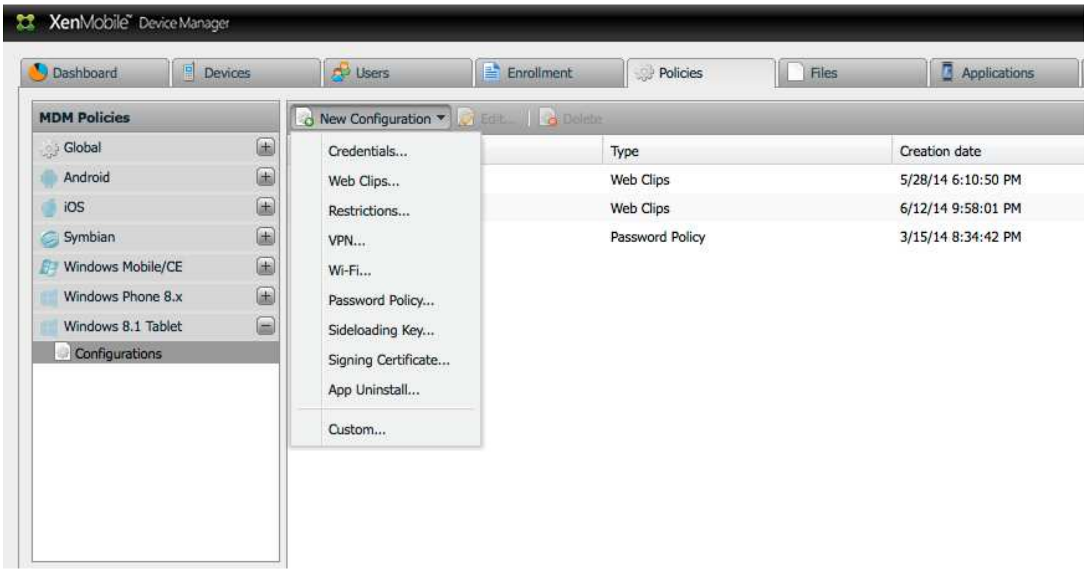
Help
You can edit device properties from the Properties tab.

Policies and Settings for Windows 8.1 Devices

With XenMobile, management and security policies and configuration settings can be pushed to a Windows 8.1 device when the device is enrolled with the MDM Server, and when the device periodically checks back in with the server. Examples of the types of policies currently supported include:

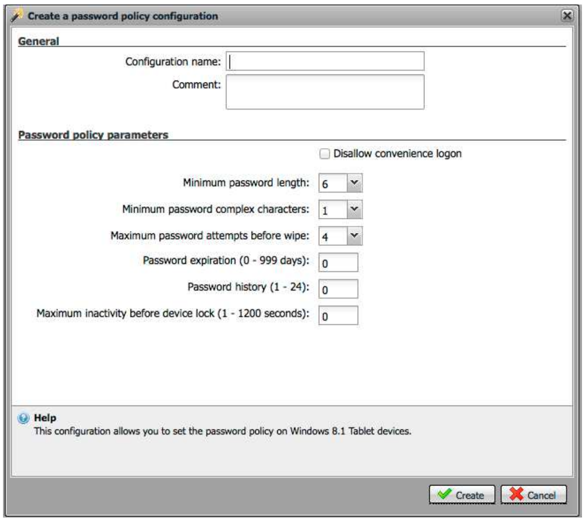
- Web shortcuts delivery
- Restrictions settings
- Password policy setting
- Credentials delivery
- Configure Device VPN
- Configure Wi-Fi Connections
- Sideloading Key
- Signing Certificate
- App Uninstall

The **“Policies”** tab is used to create corporate policies and configuration settings to be pushed to devices. The screenshot below shows the policies available for Windows 8.1 devices in XenMobile 9.0.



Type	Creation date
Web Clips	5/28/14 6:10:50 PM
Web Clips	6/12/14 9:58:01 PM
Password Policy	3/15/14 8:34:42 PM

To create a new Configuration or Policy, select the appropriate menu option from the “New Configuration” menu and fill in the displayed form with the required information. For example, to create a password policy for a Windows 8.1 device, select the “Password Policy” option from the menu and then fill in the “Create a password policy configuration” form. As shown below, you can require a password of a certain length and complexity and can specify the number of failed login attempts allowed, the password expiration in days, etc.



Create a password policy configuration

General

Configuration name:

Comment:

Password policy parameters

☐ Disallow convenience logon

Minimum password length: 6

Minimum password complex characters: 1

Maximum password attempts before wipe: 4

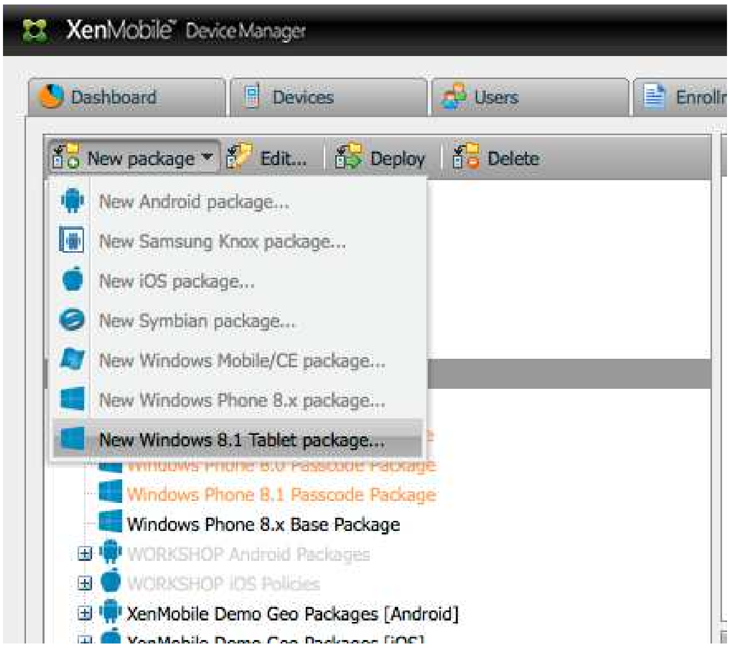
Password expiration (0 - 999 days): 0

Password history (1 - 24): 0

Maximum inactivity before device lock (1 - 1200 seconds): 0

Help
This configuration allows you to set the password policy on Windows 8.1 Tablet devices.

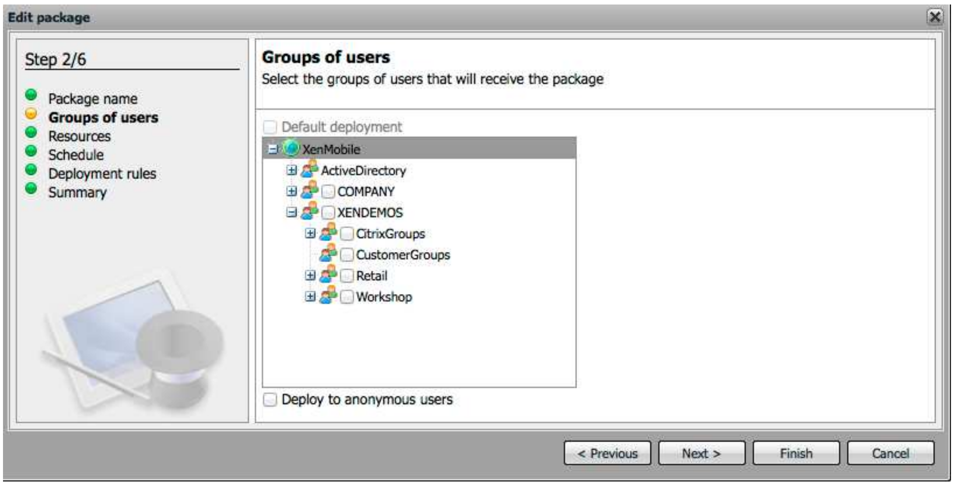
Once a policy has been defined and created, the next step is to create a XenMobile "deployment package" to specify the specific users (based on AD groups) who will have that policy pushed to their Windows 8.1 devices when the devices are enrolled. Deployment packages are created from the administration console's **"Deployment"** tab. As shown below, a simple wizard guides an administrator through the process of creating a deployment package.



XenMobile Device Manager
Dashboard
Devices
Users
Enrollm
New package
Edit...
Deploy
Delete
New Android package...
New Samsung Knox package...
New iOS package...
New Symbian package...
New Windows Mobile/CE package...
New Windows Phone 8.x package...
New Windows 8.1 Tablet package...
Windows Phone 8.0 Passcode Package
Windows Phone 8.1 Passcode Package
Windows Phone 8.x Base Package
WORKSHOP Android Packages
WORKSHOP iOS Policies
XenMobile Demo Geo Packages [Android]
XenMobile Demo Geo Packages [iOS]

The administrator first specifies that they will create a new Windows 8.1 Tablet package. Then they fill in the screens presented by the wizard to specify the Active Directory groups that the package is to be deployed to and the specific resources—MDM configuration policies, applications, etc.—that will be deployed with the package.

“Groups of users”—select the Active Directory groups that this deployment package and associated resources will be sent to.



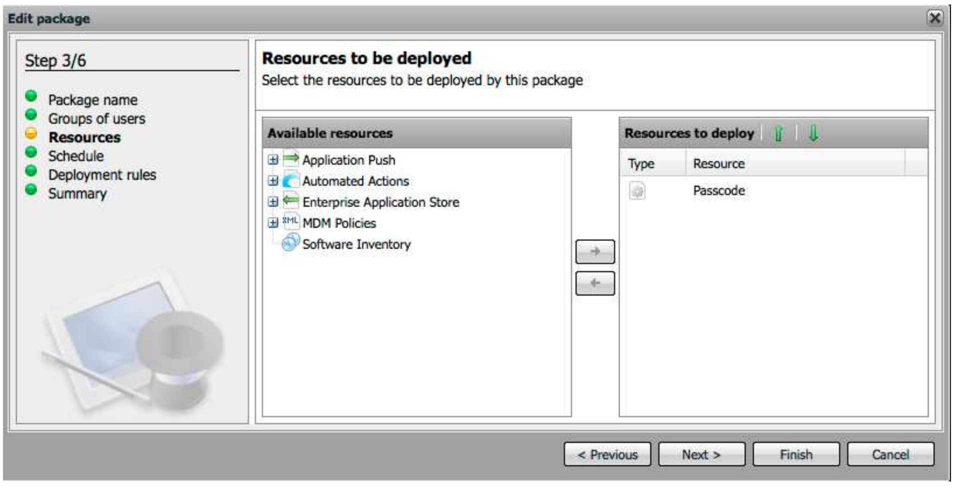
Edit package

Step 2/6

Groups of users

Select the groups of users that will receive the package

“Resource to be deployed”—specify the policies, configuration settings, web clips, automated actions, etc. to be included in the deployment package.



Edit package

Step 3/6

Resources to be deployed

Select the resources to be deployed by this package

The use of deployment packages to target different resources to different groups of users makes it extremely easy to configure the devices of different user groups differently. Different configuration settings, security policies and applications are pushed to user’s devices as required by their job function and security needs.

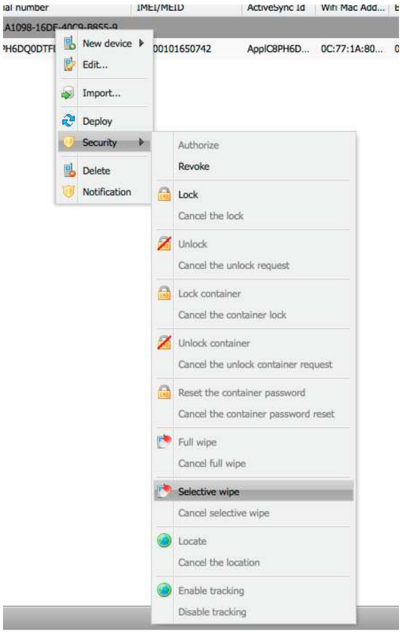
Security & Management Commands

Security and management commands can also be sent from the MDM Server management console to a Windows 8.1 device, including:

- Device lock
- Device selective wipe (un-enrollment)

These commands are useful if an employee loses a device or the device stolen, as the device can be remotely locked or even wiped to keep sensitive corporate information or networks from being accessed by someone who has access to the lost or stolen device. A "Selective Wipe" does not touch an employee's personal applications or data. It only removes the corporate configuration policies that have been pushed to the device by XenMobile.

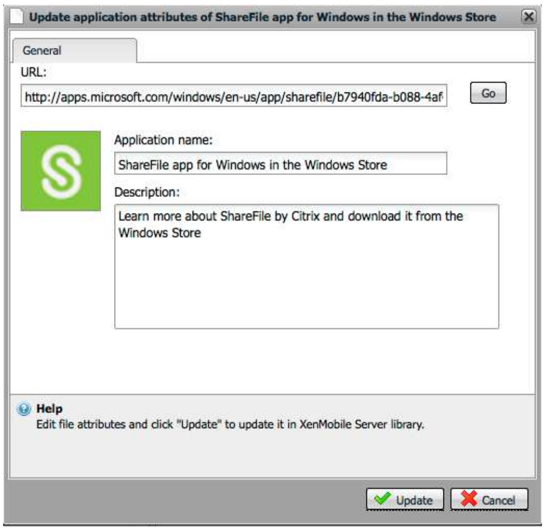
To send one of these security commands to a device, simply select the device on the **"Devices"** tab and then click the "Security" button (or right-click on the device in the list and select the Security menu option.) When the Security menu is displayed, select either a Lock command or a Selective Wipe command to be sent to the device.



Provisioning Applications

XenMobile can also push a “Corporate Application Store” web clip to Windows 8.1 devices. When a user goes to the store it will contain links to Windows applications that they can download to their device. This corporate store provides an easy way to make job-specific applications available to employees on their Surface tablets.

First, applications (links to applications) to be made available in the store are added to XenMobile from the **“Applications”** tab of the administration console. Click on the “New” button and select the “New external Windows 8.1 tablet app” menu option. Then fill in the form with the URL of the application in the Microsoft store. Hit the “Go” button to fill in the details of the application and then hit the “Add” button. This application can now be made available to users in the corporate store that is pushed to a user’s device when they enroll it with XenMobile.



Update application attributes of ShareFile app for Windows in the Windows Store

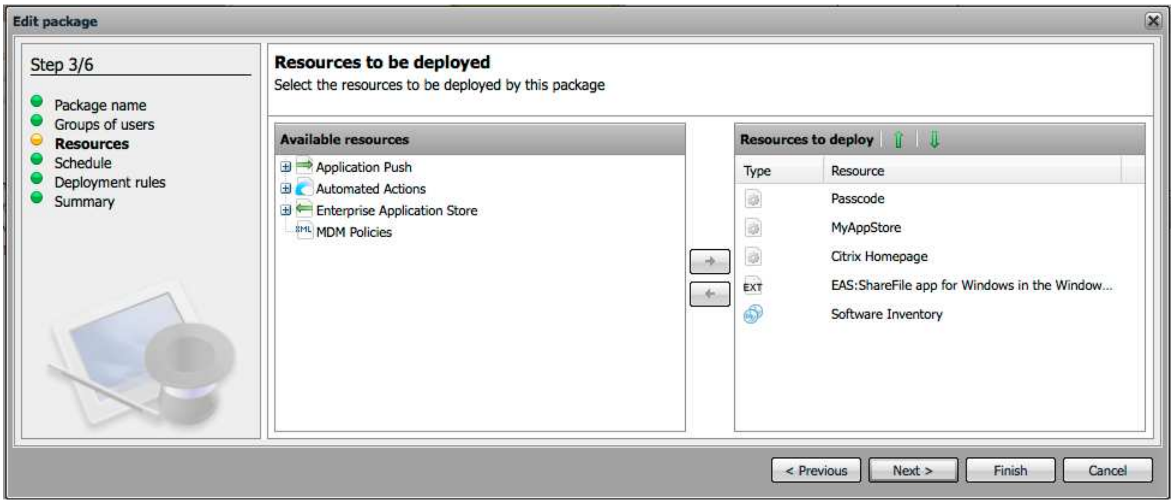
URL: http://apps.microsoft.com/windows/en-us/app/sharefile/b7940fda-b088-4af

Application name: ShareFile app for Windows in the Windows Store

Description: Learn more about ShareFile by Citrix and download it from the Windows Store

Help
Edit file attributes and click "Update" to update it in XenMobile Server library.

Next, create a deployment package that includes both the corporate store web clip (created as a policy) and also specifies the applications to be made available in the corporate store. In the screenshot below, the corporate store will make the Citrix ShareFile application available on the Surface tablet from the corporate store web clip.



Edit package

Step 3/6
- Package name
- Groups of users
- **Resources**
- Schedule
- Deployment rules
- Summary

Resources to be deployed
Select the resources to be deployed by this package

Available resources
- Application Push
- Automated Actions
- Enterprise Application Store
- MDM Policies

Resources to deploy

Type	Resource
	Passcode
	MyAppStore
	Citrix Homepage
EXT	EAS:ShareFile app for Windows in the Window...
	Software Inventory

Conclusion

XenMobile MDM provides a powerful and easy way to manage a wide variety of mobile devices, both corporate and employee-owned, from a single MDM system. With the inclusion of open mobile device management (MDM) APIs in Windows 8.1, devices such as Microsoft Surface tablets can now be managed from XenMobile in the same manner as iOS, Android and Windows Phone devices. Security policies and configuration settings can be automatically pushed to Windows 8.1 devices and the devices can be easily monitored and managed for compliance with corporate security policies.

Rev 1. M.McAuliffe