Rensselaer's Mobile Device Management (MDM) Services

Mobile Exchange (MobEx) @ Rensselaer

History of the Service

In August 2005, DotCIO announced support for BlackBerry devices under the "**BlackBerry @ Rensselaer**" (B@Re) moniker. Then, in October of 2009, DotCIO announced the next generation of Rensselaer's MDM service for Exchange users, **Mobile Exchange @ Rensselaer** (MobEx), a self-funding subscription service with an annual fee which provides secure and reliable access to DotCIO's Exchange services for BlackBerry and Apple iOS devices.

Beginning August 2012, in addition to BlackBerry and Apple iOS mobile devices, DotCIO now provides support for many devices running Google's Android OS. The **MobEx** MDM solution has been very successful, allowing DotCIO to support a large number staff and faculty with mobile devices, with more than 350 subscribers and 370 registered devices, today.

Supported Devices

Since the introduction of a service supporting mobile devices, almost 8 years ago, we have tracked the smart phone market closely. We have purchased popular and promising devices from a variety of manufacturers to evaluate for use with the **MobEx** service.

The most difficult aspect of supporting multiple devices is that of support and qualification. Many of the departmental administrators have limited access to smart phone devices and it is unlikely these support staff will be provided with multiple devices in order to familiarize themselves well enough to completely support them.

As of August 1st 2012, any currently available Apple iPhone (3Gs and newer), the iPad (all versions), any Blackberry model, Android phones running 2.3.x (Gingerbread) or greater, and Android tablets running 4.0.x (Ice Cream Sandwich) or greater are supported.

(*Please note that Pre-Gingerbread Android OS based devices are NOT supported. Android devices are supported ONLY if they are running the "Touchdown" Exchange client by Nitrodesk. Any future iPhone and Android models will be evaluated to assure they meet security requirements and compatibility with our MDM services before becoming a MobEx @ Rensselaer supported device*).

The MobEx @ Rensselaer Program

- Eligible subscribers must
  - Staff and or Faculty taking advantage of the Exchange Email Services provided by the DotCIO
  - Use only those devices supported by the MobEx @ Rensselaer program
  - Have a computer support person who will provide support for all aspects of their mobile solution.
    - In the event it is necessary, DotCIO will work directly with departmental computer support staff to address server-side issues.
  - Install the MDM agent, AirWatch, free from the app store (Android and iOS devices).
- Each individual MobEx @ Rensselaer subscriber will be charged a yearly subscription fee (**currently $100**) which will be renewed each July at the then current subscription fee. Subscription fees are not prorated or refunded.

Personally-owned devices:

- They are discouraged, but allowed to be used with the program.
- Because service-linked devices contain institute owned data, it is the responsibility of the employees who run the MobEx @ Rensselaer service to maintain control of that data and to protect the interests of the University, regardless of the terms associated with the ownership of the connected device.
- The MobEx @ Rensselaer Subscriber must acknowledge that once separated from the institute, RPI-related data on their device, personally-owned or otherwise, will be removed and the device disconnected from the Exchange service. ("RPI-related Data" includes, but is not limited to, Exchange mail, exchange contacts, Exchange calendar information, pre-configured RPI wireless access, RPI-licensed mobile applications). **Every effort will be made during a remote "Corporate Wipe" procedure, to leave personal email, personally owned applications, device settings, and other personal data, untouched.**

MDM Enforced Device Policies

The BlackBerry Policy

An IT Policy will be created on the BlackBerry Enterprise Server (BES) which will be automatically downloaded and installed on each BlackBerry. The installation of the IT Policy will define, at a minimum, the following configuration settings:

- Require a password to unlock the device
- Require a Minimum password length of 4 alpha numeric characters.
- Passwords must not contain many of the "most common" passphrases (ie "password")
- Specify a Maximum of 10 failed password attempts before the device is wiped of all data
- Specify an Inactivity time of 60 minutes
- Limit Bluetooth Discoverable time
- Require a password for enabling Bluetooth and discoverable mode
- Keep messages on the BlackBerry for a maximum of 90 days
- Specify "Owner Information" field (Even on personal devices)
- Set owner name as "Rensselaer Polytechnic Institute (Even on personal devices)
- Specify the Home Page Address as: http://mobi.rpi.edu/blackberry
- Specifies that the device file system is encrypted (With the exception of Multi-media directories).

Apple iOS Device Policies

IT Policies will be pushed from our AirWatch MDM server and communication between the MDM server and the Apple device will be done through the use of the AirWatch agent, a free App which users will be required to download from the App store and install on their iPhone or iPad as part of the configuration process. The installation of IT Policies and the MDM agent will define and verify the following configuration settings are in place:

- Require a password to unlock the device
- Require a Minimum password length of 4 numeric characters
- Specify a Maximum of 10 failed password attempts before the device is wiped of all data
- Specify an Inactivity time of 60 minutes
- Force SSL encryption between the device and the Exchange server
- Install an 802.1x Wi-Fi configuration for use on RPI's wireless network
- Install a set of configuration options for external VPN access to RPI's internal network
- Install a Web Shortcut on the iPhone desktop linking to http://m.rpi.edu

Android Device Policies

IT Policies will be pushed from our AirWatch MDM server and communication between the MDM server and the Android device will be done through the use of the AirWatch agent, a free App which users will be required to download from the Google App store and install on their Android as part of the configuration process. The installation of IT Policies and the MDM agent will define and verify the following configuration settings are in place:

- Require a password to unlock the device
- Require a Minimum password length of 4 numeric characters
- Specify a Maximum of 10 failed password attempts before the device is wiped of all data
- Specify an Inactivity time of 60 minutes
- Force SSL encryption between the device and the Exchange server
- License and Configure Touchdown by Nitrodesk (The ONLY supported Exchange email App)
- Install a Web Shortcut on the Android desktop linking to http://m.rpi.edu

Advantages of being connected to MobEx

- Data is delivered in real-time and without carrier imposed mailbox quotas
- Users have wireless, synchronized access to their RPI Exchange email, calendar, and contacts
- Since all data storage is local to RPI, Rensselaer support staff can directly assist users if difficulties arise
- DotCIO can provide a variety of evaluation devices, with service, to users who are considering MobEx @ Rensselaer
- MobEx @ Rensselaer provides end-to-end encryption between the wireless handheld and the Exchange mail server
- Data on secure digital memory cards can be encrypted to prevent unauthorized access by another device.
- If a supported handheld is lost or stolen, Rensselaer support staff can remotely initiate a command that erases all data and eliminates the potential of exposing sensitive information.

- All MobEx @ Rensselaer servers are housed at Rensselaer, secured behind multiple layers of firewalls.
- Security Policies are administered and distributed remotely by the MobEx @ Rensselaer administrator.
- The MobEx @ Rensselaer service extends Rensselaer's security policies to the wireless device and provides users and support Administrators with tools to manage many aspects of the mobile experience.
- To secure information stored on all supported mobile devices, pin code authentication is mandated through IT policies applied to all connected devices.
- Password authentication is limited to ten attempts after which point, data on the device is automatically erased.
- Local storage of data (messages, address book entries, calendar entries, memos and tasks) is, or can be, encrypted.

Conclusion

We recognize that some people may prefer a mobile device other than those currently supported by the service. We acknowledge that MobEx @ Rensselaer is not better than all of the alternatives in every way. However, MobEx @ Rensselaer is presently the best way for Rensselaer to provide Exchange users with supportable, affordable, reliable, and sustainable mobile access, in a manner which protects the interests of Rensselaer and its user community.

The overwhelming consumer success of Google's Android OS has motivated us to evaluate each new Android OS, and to now qualify additional Android devices as MobEx @ Rensselaer devices.

Next Steps

In order to start synchronizing your approved device with Exchange, you should begin by contacting a member of your computer support team, who will work with you. Your computer support person can assist you in configuring your device in the correct way, help verify that you are connected to the service, and assist in troubleshooting any issues and answer any questions you may have.

This document was last updated: Thursday, October 04, 2012