Mobile devices are widely used by faculty, staff, students and other authorized individuals to access a variety of MUSC systems that contain sensitive data, including administrative and financial records, educational records and protected health information. While mobile access can provide valuable benefits, there is a significant risk of unauthorized access to sensitive MUSC data if a mobile device is lost or stolen or otherwise leaves the control of its owner or authorized user.

**Who:** Mobile Device Management is required for ALL users who connect to the MUSC Exchange server (MUSC email) from a smart phone.

**Why:** By requiring Mobile Device Management (MDM) software on smartphones, the following goals will be achieved:
- Force Password Lock
- Require Inactivity Timeout
- Enforce Encryption of MUSC data including email, contacts and calendar information.
- Push `<muscsecure>` wireless and VPN settings to our users’ devices and remove them if necessary.
- Push Exchange Email, Contacts and Calendar settings to users’ devices and remove them if necessary.
- Add the ability to Wipe, Selectively Wipe MUSC Data only, locate lost devices if users choose to allow their device to be located. The physical security of mobile devices must be maintained at all times. In particular, these devices should not be left unattended in any location where loss or theft or any access to the device by an unauthorized party would be a reasonably anticipated and avoidable risk.

If devices are lost, users will have the ability to log into a self-service portal at [http://www.musc.edu/myphone](http://www.musc.edu/myphone) and do the following:
- Lock their device
- Locate their device (If they have location services turned on and GPS enabled on their device)
- Wipe their device completely
- Wipe only MUSC data from the device (Exchange Email, Exchange Contacts, Exchange Calendar, MUSC VPN Settings, muscsecure wireless settings, passcode policy)

*Please Note: MDM does NOT allow administrators to see users' private data stored on their phone such as messages in MUSC or personal email accounts, pictures, videos, phone calls, and text messages. MDM does allow administrators to see device data such as Battery Life, UDID, Phone Number of Device, Location of Device (only with written permission of the user when users allow their device to be located), Applications installed on the device, and Passcode and Encryption Compliance.*

**ALL users who connect to the MUSC Exchange server from their phone will be required to install the Xen Mobile MDM client.**

Please email any questions and/or suggestions to endpointsecurity@musc.edu.
Configuring MDM:

1. On the main screen of your Windows 8 phone, tap the right arrow button (or swipe to the left).

2. Select Settings.

3. Select Company Apps.

4. In the Company Apps screen, tap Add Account.

5. In the next Company Apps screen, enter your NetID and password, then tap sign in.

6. On the next screen, enter \texttt{https://mdm.musc.edu:8443/zdm/wpe}.

7. Tap Sign In.

8. You may see a screen that asks if you want to continue if the certificate is unknown to the device. Click Continue.

9. When the account is added, click Done.

10. You will receive a prompt to create a passcode for your phone.

Configuring Email:

1. On the main screen of your Windows 8 phone, tap the right arrow button (or swipe left).

2. Select Settings.

3. Select Email+Accounts.

4. In the Email+Accounts screen, tap Exchange.

5. In the next Email+Accounts screen, enter your NetID and password, and then tap sign in.


7. Tap sign in. You may be prompted for the domain; enter clinlan.local.