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 smartphone.

**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.
Getting Started: iOS

**Please have your Apple ID password accessible.**

Xen Mobile is going to configure your Exchange, VPN and muscsecure wireless settings. However, you will first need to remove your current settings. **Note: If you do not have these settings configured at all, please proceed to the "Installing MDM on your Device" section.**

**Removing Current Settings**

There are two different procedures to remove these settings depending on how they were installed. Please check each of the procedures below.

- **Procedure 1** (if you configured Exchange, VPN and muscsecure wireless from the profile available on NST Wiki):
  Remove the profile by going to **Settings → General → Profiles → Locate the MUSC profile and Press Remove → Remove**

- **Procedure 2** (if there are no profiles present and settings were manually configured):
  Remove Exchange email by going to **Settings → Mail, Contacts, Calendars → Select the MUSC Exchange Account → Press Delete Account**
  Remove muscsecure wireless by going to **Settings → Wi-Fi → muscsecure → Press Forget this Network → Forget**
  Remove VPN by going to **Settings → General → VPN → Press your VPN Configuration → Press Delete VPN → Delete** (if MUSC VPN is not listed, continue to steps below)

**Installing MDM on your iOS Device**

1. From your mobile device, open the **App Store**, then search for **Secure Hub by Citrix**.
2. Press the **cloud/arrow icon** to install the app.
3. Once installed, open the **Secure Hub** app.
4. Enter your **NetID@musc.edu** in the blank provided and press [Next]. **Note** - Do not use your email address unless it is the same as your NetID. For Example: If your NetID is jct14, register for MDM with **jct14@musc.edu**. DO NOT use just your NetID. Make sure it is followed by “@musc.edu”.
5. Enter your NetID password and press [Sign on].
6. The browser will open. Press **Install → Install → Install → Done** (You will be prompted to enter your PIN if you already have one set)
7. Press **Install → Install → Install → Trust → Done** **Please Note**: Xen Mobile 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. The warning message you see is a generic Apple message.
8. Secure Hub will automatically complete the rest of the enrollment process.
9. After you see **[Your device is successfully enrolled.]** Press the home button (round button on the bottom of your phone.) Two new apps will now be on your screen **Secure Hub and Self-Serve**.
10. If you do not already have a PIN on your phone, you will receive a prompt that states “You must set a passcode within 60 minutes.”
11. Press **Continue. Enter a PIN. Press Continue. Re-enter your passcode for verification. Press Save.**
12. Press the **Mail Icon** on your iPhone’s Home Screen. You will be prompted to enter your password for Exchange. **Enter your MUSC NetID Password. Press OK.** Your Exchange Mail, Contacts and Calendar will begin to download momentarily.

**Note: If your Calendar does not show up when your email does:**

1. Open your Calendar App
2. Click **<Calendars>** in the top left corner
3. **Make sure that “All Exchange” is checked. If it is not, Click the word “Exchange”** (It will add a check mark next to this Calendar and your calendar should be populated once you click <Done>.)