



University of Connecticut
Health Center

UCHC IT DEPARTMENT

BYOD - Provisioning for Android Enterprise

A Provisioning Guide for Employee-Owned Android Devices using the BYOD portal at UCHC

Android Enterprise Version 1.0

*Please note: Android versions can differ greatly between models and manufacturers - this tutorial **MUST** be viewed as a general guideline only. Please contact the Help desk at ext. 4400 to have any questions directed appropriately.*



Note the following items before continuing:

- There is an excellent resource available to assist UCHC users with the provisioning process online at <http://its.uchc.edu/Help/BYOD.aspx>
- A native email experience may be possible if you have a Samsung Galaxy device. Contact mobile device services for details.
- If you have an existing UCHC Exchange Account – you must remove it prior to provisioning.
- Similar Android versions can differ greatly between phone models and manufacturers.
- A security warning may display if you attempt to access the byod.uchc.edu website. Continuation will not harm your phone.
- You will need to enter the server name *mobile.uchc.edu* if prompted.
- You will need your Domain Name and Password to continue.
- You will need to decide and have a thorough understanding of your device's capability and intent to access and utilize confidential information.
- Choose **NO** if prompted to save your domain credentials.
- The self-registration experience on any Android phone can, and will be different, even on two identical phones.
- You will need to accept any certificates presented.
- The following requests may display and must be answered as indicated below for MobileIron to function properly.
 - A.) MobileIron Administration (**Activate or Enable**)
 - B.) Device Management (DM) Utility functionality (**Install, Enable and or Activate**)
 - C.) Certain DM Applications are embedded on some Android phones and as a result are not native to the Google Play Store. You may be prompted at some point to **Allow unknown sources** (*Check box must be selected, but can be deselected after installation of DM utility.*)
 - D.) Device Manufacturer Administration [i.e., Samsung Knox or Motorola] (**Activate or Enable**)
 - E.) You will need to create a pin consisting of at least six digits if you select **Yes** to confidential status.

Important: Please "forget" your UConn Health Secure Wi-Fi settings before starting. This can be accomplished by going to your connections and then Wi-Fi and choose advanced. From there you can choose network management and then select and forget each instance. You will need to temporarily enable cellular data in order to move forward and once completed, MobileIron will automatically log onto the UConn Health Secure Wi-Fi on your behalf.

The following example details the primary components of a generic Android BYOD registration using a LG G3, Samsung Galaxy S6,7 and S8. Actual illustrations will vary by device and manufacturer).



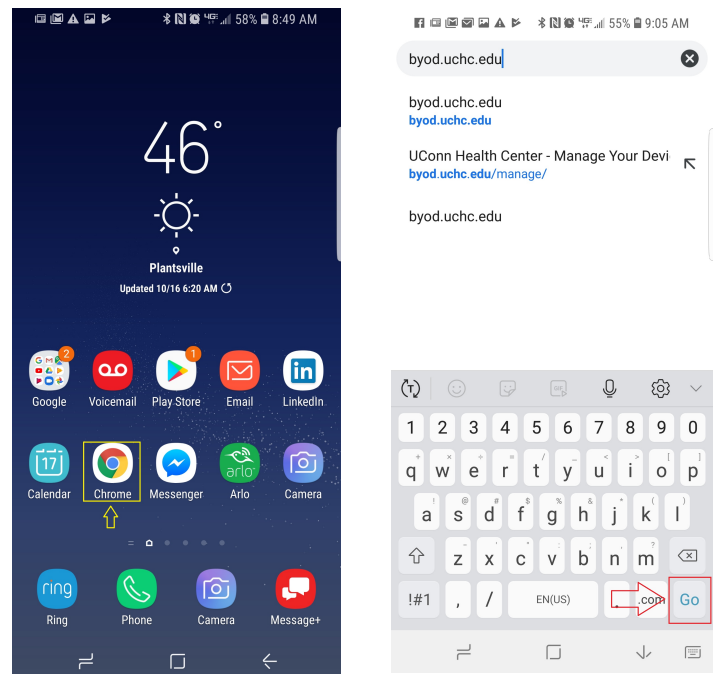
Please be sure to have the latest version of Android installed

ACTION	RESULT/COMMENT
--------	----------------

Note: You will need to be added to an Android Enterprise label via the MobileIron Core Server prior to registration.

Please contact the help desk on ext4400 and ask that a work order requesting Android Enterprise be created for the mobility team. A mobile support professional will add you and then contact you to confirm and offer assistance if needed.

1. Open your browser from the home screen.
2. Type **https://BYOD.uchc.edu** in the address bar and choose **Go** on the phone keyboard.

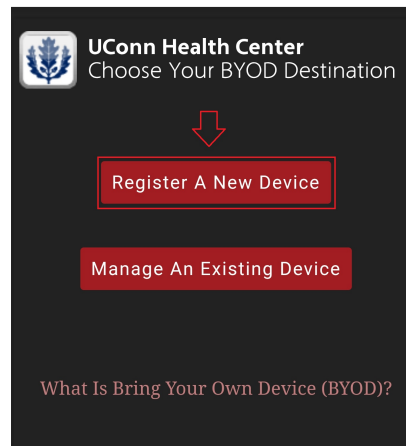


RESULT/COMMENT

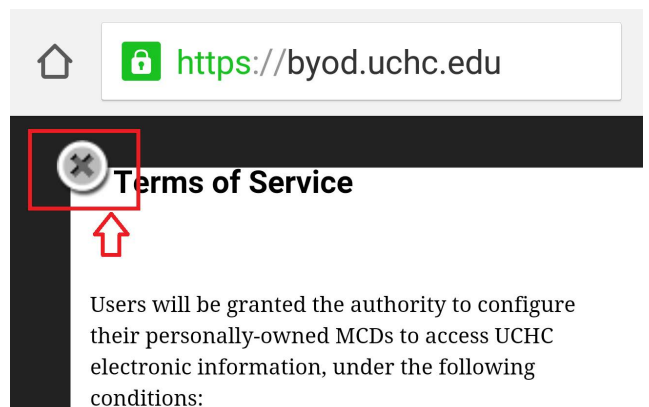
3. Choose Register A New Device.

71% 10:05 AM

https://byod.uchc.edu



4. Read the End User Agreement and then close the window by choosing the X next to Terms of Service.

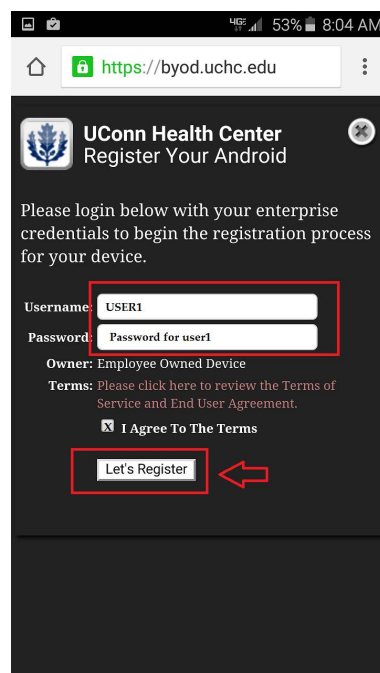


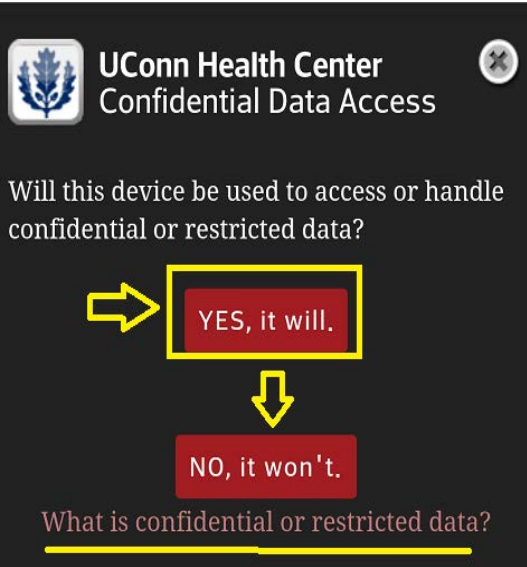

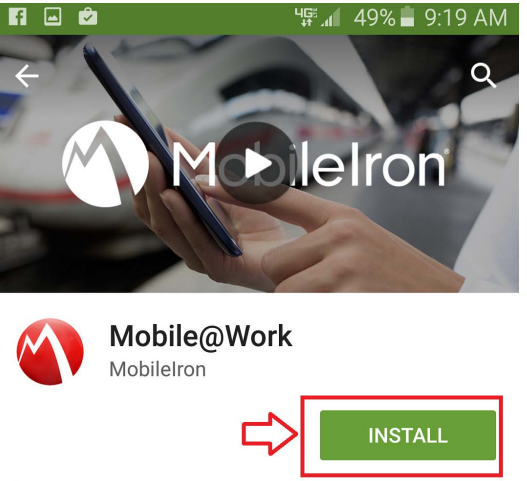
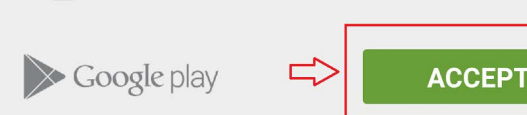
5. The **Register Your Android** screen displays.

Enter your network credentials in the **Username** and **Password** fields.

(These are the credentials used to sign into your office computer.)

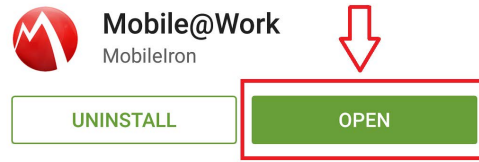
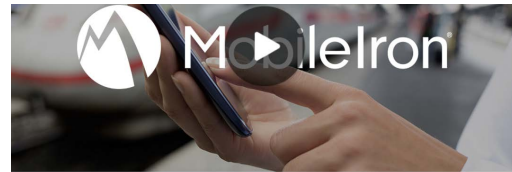
Choose **Let's Register**.
(If a **Confirm** window displays prompting you to save your password, select **Never**.)



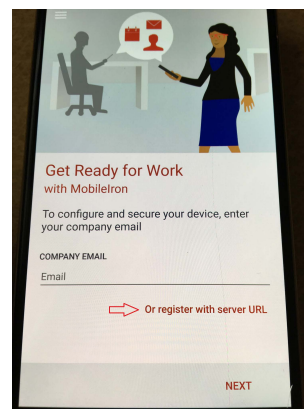
ACTION	RESULT/COMMENT
<p>6 The Confidential Data Access screen displays.</p> <p>① Select YES if the device is exposed to confidential data.</p> <p>② Select NO if the device is NOT exposed to confidential data.</p> <p>(You can click the <i>What is confidential or restricted data?</i> link if you need help determining your type of data access.)</p>	
<p>7. Choose Get App on the next screen.</p>	
<p>8. Choose Install when the MobileIron client application screen appears.</p>	
<p>9. Choose Accept.</p>	

RESULT/COMMENT

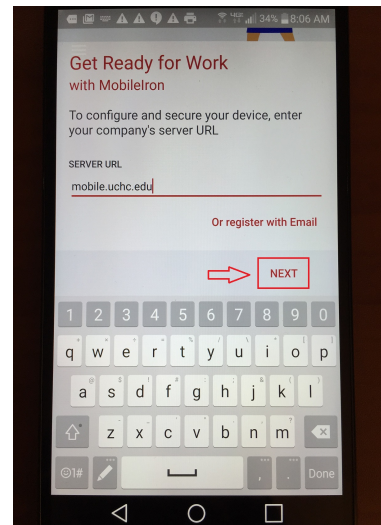
10. Choose **Open** once the installation is completed.



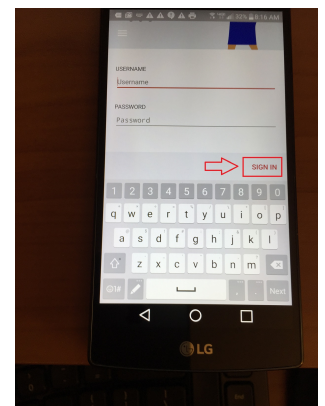
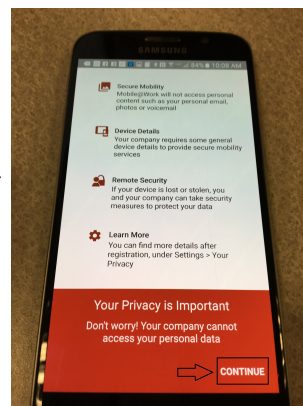
11. Choose "**Or register with server URL**".



12. ① Enter **mobile.uchc.edu** in the server address field if it has not already populated.
② Choose **Next**.



13. Read the privacy statement and choose **CONTINUE**.
- Enter your network credentials in the User Name and Password fields. Choose **SIGN IN**.
- (These are the same credentials used to access your office computer.)*



ACTION

RESULT/COMMENT

14. Choose Continue to initiate device administration if you are prompted to do so.

15. Choose Activate to continue.
(Please note that if you have a Samsung Galaxy S6 or newer, you may be prompted to confirm the Knox privacy policy.)

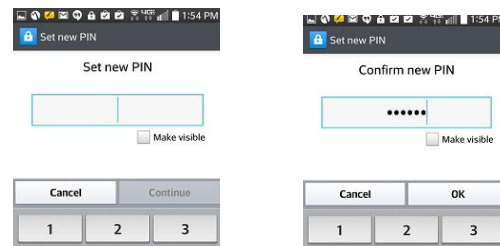
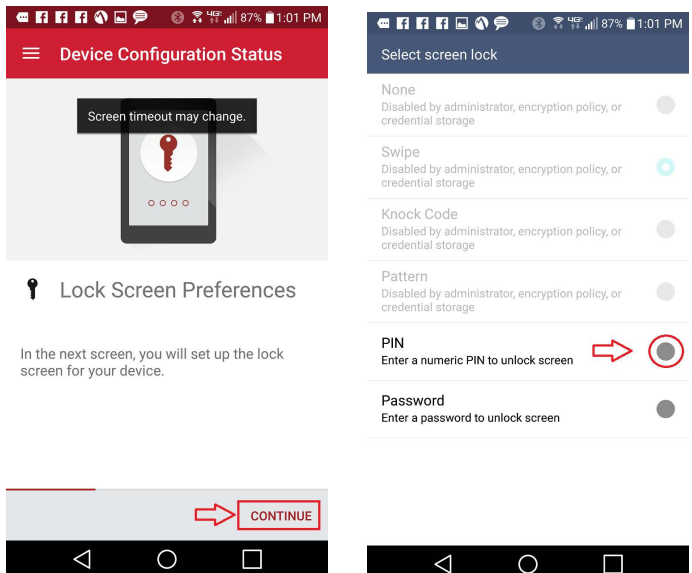
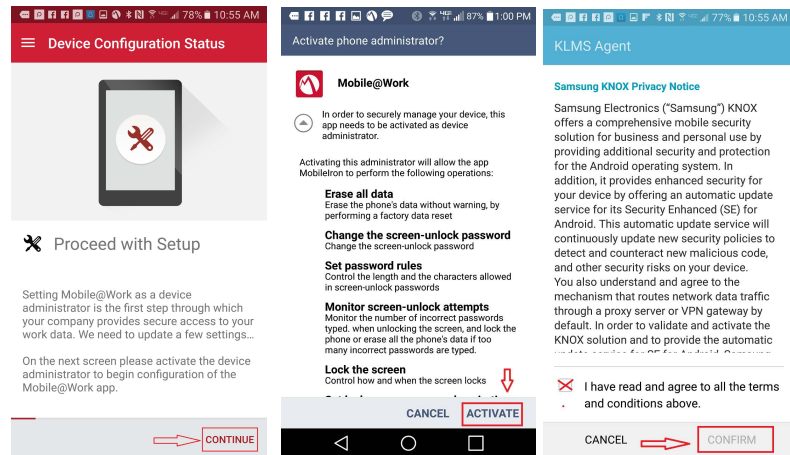
16. Choose continue on the lock configuration screen if one appears.

Please note that if your device already has a password established you will not see this prompt and you can skip to step # 19 below.

17. Choose PIN or Password and then see step #18 below.

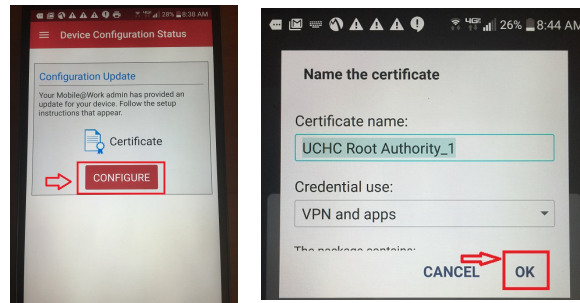
The Password option is a higher level of security as it prompts you for an alphanumeric lock code. The PIN option (recommended) will prompt you for a numeric code. Choosing the Password option will also unnecessarily encrypt the entire phone.

18. Enter your new PIN and then confirm your entry when the pin selection screen appears.



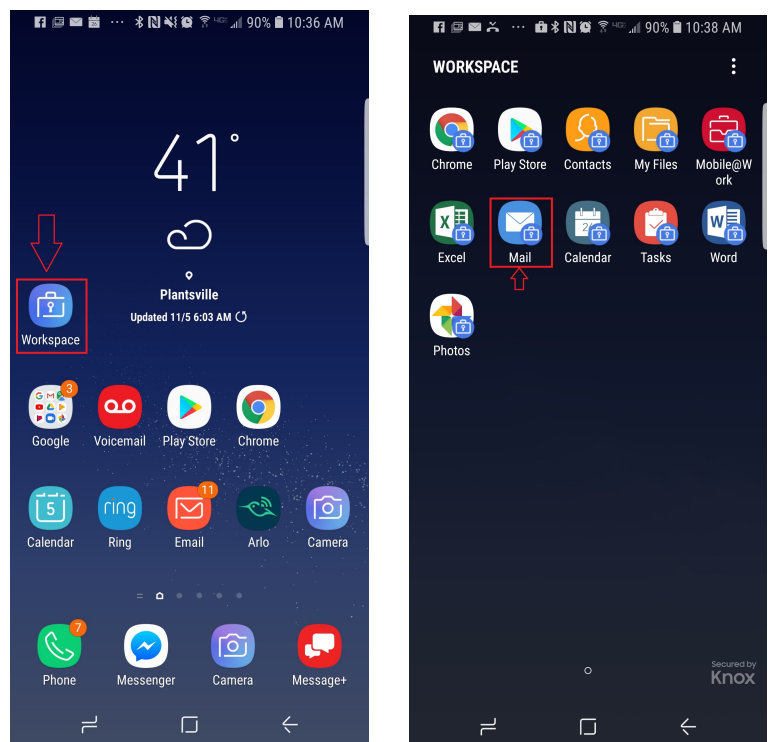
ACTION	RESULT/COMMENT
--------	----------------

19. Choose **Configure** and then **OK** if prompted by any configuration update screens that may appear.



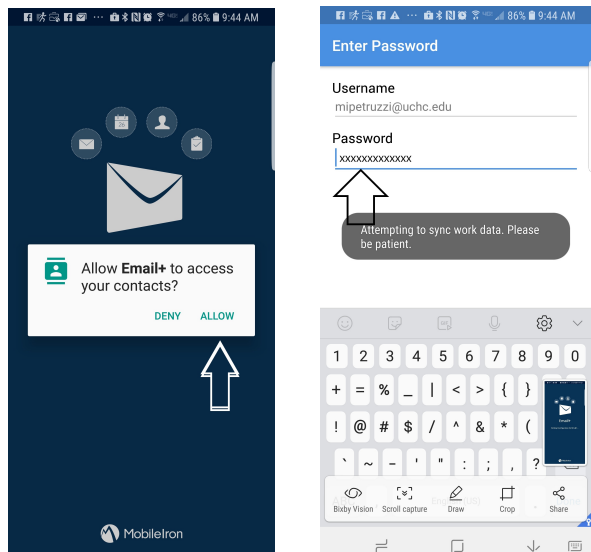
20. Locate the Workspace folder Icon in your application list and move it to your home screen once you have allowed MobileIron to finish processing.

*Note: It can take up to 10 minutes for **Workspace** to appear. Some phone versions will not populate the workspace icon, setting the work space icons into the normal application list. You can identify them by the small lock symbol on the lower right hand side of the icon. Other phones will label the **Workspace** folder as simply, **Work**.*



21. MobileIron Email + Configuration Status displays. Choose **Allow or Configure** when prompted during set up of Email.

22. Enter your email password when prompted and your email will populate after a brief period of synchronization.



Congratulations! You have successfully provisioned your device for email, calendar and Wi-Fi acquisition!

Revision History

Please itemize all *material* changes to this document in the table provided. It is not necessary to document modifications encompassing only spelling, punctuation, or other minor, non-material edits in the Revision History table.

Version	Date	Description	Author
1.0	11/5/2018	Document creation	M.Petruzzi