## **UCONN** HEALTH

### **UCHC IT DEPARTMENT**

## **BYOD - Provisioning an Android Phone**

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

Version 3.0

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.

## UCONN HEALTH

## Note the following items before continuing:

- There is an excellent resource available to assist UCHC users with the provisioning process online at <a href="http://its.uchc.edu/Help/BYOD.aspx">http://its.uchc.edu/Help/BYOD.aspx</a>
- A native email experience may be possible of you have a Samsung Galaxy device. Contact mobile device services for details.
- If you have an existing <u>UCHC</u> 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 <u>byod.uchc.edu</u> 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.) MI Administration (Activate)
  - B.) Device Management (DM) Utility functionality (Install 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)
  - E.) You will need to create a pin consisting of at least six digits if you select *Yes* to confidential status.



The following example details the two 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).

- 1. Install TouchDown for Smartphones (Do not open the Application)
- 2. Install the MobileIron@Work Client Application

#### TouchDown

The TouchDown application downloads from the Google Play Store and downloads automatically once selected.

ACTION	<b>RESULT/COMMENT</b>
1. Access the <i>Google Play Store</i> from the <b>Home</b> screen.	Email Camera Play Store Google
2. Search in the store for <u>TouchDown</u> <u>for Smartphones.</u>	★ touchdown       Exchange by TouchDown Key     :       A3 ★     19.69       TouchDown For Smartphone     :       A0 ★     FREE       TouchDown HD     :
3. Download the application by selecting <i>Install</i> .	TouchDown for Smartphones         NortorMobile         Image: State of the sta
4. Choose <i>Accept</i> App permissions if prompted.	Couple Down for Smartphones needs access to     Device & app history     dentity     Contacts     SMS     Mein/Files     Multi-Files     Multi-Files     Whi-Fi connection Indemtion     Device & all     Device to all     Device
5. Touchdown will begin downloading.	TouchDown for Smartphones       NortonMobile       4.66MB/9.13MB     51%
6. Be sure <u>not</u> to choose open once the install has been completed. Go to your home screen once the download has finished.	TouchDown for Special-200
	NortonMobile

UNINSTALL

# HEALTH



You MUST successfully install the *TouchDown* application beginning on page 1 before initiating the MobileIron installation process.

#### ACTION

- 7. Do not open the Touchdown application. Choose the Home icon or physical Home Button depending upon the model of phone.
- 8. The Touchdown application should be visible on the home screen and will eventually become your short cut to UCHC Exchange mail.
- 9. Open your internet browser by choosing the browser icon on your home screen.
- 10. Type https://BYOD.uchc.edu in the address bar and choose go.

#### **RESULT/COMMENT**









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

11.

- 13 The Register Your Android screen displays.
- Enter your network credentials in the 1 Username and Password fields.

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

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



#### ACTION

- 14. The Confidential Data Access screen displays.
  - Select **YES** if the device is exposed to confidential data.

1

Select NO if the device is NOT exposed to confidential data.

> (You can click the **What is** confidential or restricted data? link if you need help determining your type of data access.)

- 15. Choose *Get App* on the next screen.
- 16. Choose *Install* when the MobileIron client application screen appears.

#### **RESULT/COMMENT**



UConn Health Center Confidential Data Access

X

Will this device be used to access or handle confidential or restricted data?











17. Choose Accept.



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



OPEN

<sup>19.</sup> Choose *Or register with server URL*.



NEXT

ertyuid dfghjk xcvbnm

UNINSTALL

- 20. Enter mobile.uchc.edu in the server address field if it has not already populated.
  - <sup>2</sup> Choose Next.

21. 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**

22 Choose *Continue* to initiate device administration

Choose Activate to continue. Please 23. note that if you have a Samsung Galaxy S6 or higher you may be prompted to confirm the Knox privacy policy.

#### 🛥 🖸 🖬 🖬 🗖 💷 🗛 \* 🕅 1 🖷 🖪 🖪 🖬 🖬 🕥 🗭 🛛 🕄 🏋 🔐 87% 💼 1:00 F 📾 🖸 🛱 🛱 🖸 🗉 🖛 🕸 🕅 🎖 🐃 📶 77% 🖹 10:55 Device Configuration State Mobile@Work Samsung KNOX Privacy Notice Samsung Electronics ("Samsung") KNOX offers a comprehensive mobile security solution for business and personal use by providing additional security and protection In order to securely manage your device, this app needs to be activated as device administrator. × Activating this administrator will allow the app MobileIron to perform the following operations: for the Android operating system. In addition, it provides enhanced security for your device by offering an automatic update Erase all data Erase the phone's data without warning, by performing a factory data reset service for its Security Enhanced (SE) for service for its Security Enhanced (SE) for Android. This automatic update service will continuously update new security policies to detect and counteract new malicious code, and other security risks on your device. You also understand and agree to the mechanism that routes network data traffic through a proxy server or VPN gateway by default. In order to validate and activate the KNOX solution and to provide the automatic Change the screen-unlock password Change the screen-unlock password X Proceed with Setup

**RESULT/COMMENT** 

Setting Mobile@Work as a device administrator is the first step through which your company provides secure access to your work data. We need to update a few settings... On the next screen please activate the device administrator to begin configuration of the Mobile@Work app.

CANCEL

 $\triangleleft$ 

Set password rules Control the length and the characters allowed in screen-unlock passwords

Monitor screen-unlock attempts Monitor the number of incorrect passwords typed, when unlocking the screen, and lock the phone or erase all the phone's data if too many incorrect passwords are typed.

Lock the screen Control how and when the screen locks

0

<ul> <li>I have read and agree to all the terms</li> <li>and conditions above.</li> </ul>	
CANCEL CONFIRM	

24. Choose Continue on the Lock Configuration screen that appears.

*Please note that if your device already* has a password established you will not see this prompt and you can skip to step #27 below.

- 1	🛱 🛱 🔇 🖬 🗩 🔞 🛱 🌿 📶 87% 💼 1:01 PM
≡	Device Configuration Status
	Screen timeout may change.
۱	Lock Screen Preferences
In the	e next screen, you will set up the lock en for your device

25. Choose PIN or Password and then see step #26 below.

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



0 🗆

## HEALTH

#### ACTION

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

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

28. The MobileIron Device Configuration Status displays. Choose *Continue or Configure Email depending on phone model.* 



**RESULT/COMMENT** 

🖃 🕼 💋 📾 🗘 🏛 🛍 🛍 🤶 🍀 📶 📘 1:54

Confirm new PIN

.....

2

• • • • • A A A O

Certificate name:

Credential use: VPN and apps

Name the certificate

UCHC Root Authority\_1

CANCEL

3

49 , 1 26% 8:44 AM

ок

Cance

🔜 🚳 💋 📾 🛱 🏛 🛍 😤 🎬 💼 1:54 PN

Set new PIN

2

ork admin has provided a device. Follow the setup

👌 Certificate

1

Makev

3

- 29. The Touchdown Quick Configuration screen will display the **License Agreement**
- 30. Please read and Accept the License Agreement when prompted. Make a selection as to if you are willing to share diagnostic data and then choose *Continue*.
- 31. TouchDown will automatically begin synchronizing your Outlook email and calendar. Mail notifications will display in the Android notification drop down and an audible notification is also initiated when mail arrives.

Your Android phone is now in compliance.



Congratulations! You have successfully provisioned your device!

## HEALTH

#### **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	12/14/2012	Document creation	S. Trites
2.0	09/15/14	Version 2.0	M. Petruzzi
2.1	04/14/18	Version 2.1	M. Petruzzi
2.1.1	08-26-15	Version 2.1.1	M.Petruzzi
2.1.2	09-21-16	Version 2.1.2	M. Petruzzi