1. Microsoft Intune

1.1. Overview

Microsoft Intune is a Mobile Device Management solution that is designed to keep sensitive data and resources protected. As part of this implementation, enrollment of mobile and tablet devices is a requirement to access Office 365 resources (Email, etc). This guide is designed as a How-To for enrolling mobile and table devices. This guide is not designed as a troubleshooting guide for errors during the enrollment process. This guide also provides instructions on installing and configuring Outlook for email access.

Once enrollment is complete, IT will be able to manage limited aspects of the mobile and tablet devices for protection purposes only. Access to personal apps and data will not be lost and there is no need to manually configure company network or email connections. All private aspect of the mobile and tablet device remains intact and is not accessible by IT. The following is a list of benefits of device enrollment:

- Access the company’s network.
- Access email and other work files.
- Reset mobile and tablet devices to factory settings if it is lost or stolen.
- Automatically configuration of company email accounts.
- Get company apps from the Company Portal.

![Diagram of Company and Personal applications on a mobile device]
1.2. Privacy Overview
The following image covers what IT is able to see on the mobile or tablet device:

We care about your privacy
IT cannot see this type of information on your phone or tablet:
- CALL HISTORY
- LOCATION
- TEXT MESSAGES
- CAMERA ROLL
- PERSONAL EMAIL, CONTACTS, AND CALENDAR
- PERSONAL DATA
- WEB HISTORY
- PERSONAL APPS

IT can see this type of information on your phone or tablet:
- OWNER
- MODEL
- DEVICE NAME
- OPERATING SYSTEM
- SERIAL NUMBER
- COMPANY APPS
- MANUFACTURER

Your privacy is important to us!

1.3. Management Overview
The following are security changes of the mobile or tablet device after enrollment is complete.

- Device will be encrypted if it is not already.
- A pin passcode will be enabled if it is not already or does not meet complexity.
- Screen time out (i.e. 5 minutes) and requires passcode to login
- Passcode changes every X amount of days
- Passcode must be minimum length (4)
• Cannot use the last 3 passcodes
• Device security (block apps from unknown sources, require threat scan on apps)

Note: Jailbroken devices are not allowed to enroll.

Note: Un-Enrollment of the device removes the security enforcements which allows the device to be set back to the original preferences.

2. Enrollment Instructions

2.1. Android Enrollment

Prior to starting the enrollment process charge the mobile or tablet device. If the device is connected to the SLUCare Users wireless network, disconnect to use cellular access prior to starting.

This process is only for Android versions 5.0 and higher, do not start this process if the Android OS version is less than 5.0. If the Android OS version is less than 5.0 upgrade before starting the process.

Note: Android screens vary based on OS versions and the screens in this document may not appear exactly as the device being enrolled.

1. Select Play Store from the Home screen

2. Type Intune in the Search bar, select Intune Company Portal
3. Select Install

Note: After downloading the icon displayed is “Company Portal” on the home screen

4. Select Open after the download is complete

5. Select Sign In to begin the enrollment process

1. Enter your health.slu.edu provided email address (example: joe.smith@health.slu.edu) Note: After an email address is entered, selecting the password input redirects to the SLU login.
2. After redirecting to mySLU enter your SLU ID and password (example: smithjb)

3. If prompted for additional authentication follow the prompts to authenticate

4. If text authentication was utilized enter the verification code sent and select Submit

5. Proceed to Enroll the device by selecting Begin
6. Select Continue

Why enroll your device?
When enrolled, you'll be able to:
- Access the company's network
- Get company apps from the Company Portal
- Remotely reset your phone to factory settings if it is lost or stolen
- Automatically configure your company email account

More information about enrolling your device

CONTINUE

7. Select Continue

We care about your privacy.
- IT admin cannot see this on your device:
  - Call and VoIP history
  - Location
  - Email and text messages
  - Contacts
  - Passwords
  - Calendar
  - Camera roll

- IT admin can see this on your device:
  - IMEI
  - Serial number
  - Operating system
  - App names
  - Owner
  - Device name
  - Manufacturer

CONTINUE

8. Select Enroll

What comes next?
When you tap Enroll, your device will ask you to do one or more of the following:
- Activate device administrator permissions
- Confirm the device privacy policy
- OK the certificate prompt
- Allow phone permissions and other permission requests by Company Portal (If the app never makes phone calls)

Tap Enroll to proceed.

More information about enrolling your device

CONTINUE

ENROLL

9. Select Allow

What comes next?
When you tap Enroll, your device will ask you to do one or more of the following:
- Activate device administrator permissions
- Confirm the device privacy policy
- OK the certificate prompt
- Allow Company Portal to make and manage phone calls?

ALLOW DENY
10. Select Activate

11. Select the device category that best fits. Select Done to continue.

12.1 Green check indicates the device successfully enrolled. Select Continue to complete the device compliance

13. Expand each category to resolve the compliance issues. Each item contains a “How to” link, for further instructions.
14. A passcode is required to resolve, Select the Home button, browse to Settings -> Security -> Screen Lock -> Pin

15. Enter a new passcode (Note: Simple passcodes are not allowed, i.e. “1111”). Select Continue

16. Re-enter the passcode for acceptance. Select Save to complete

17. Make the desired selection at the Notifications prompt, Select Done
18. Return to the Company Portal and select Check Compliance to see the outstanding compliance issues left to complete.

19. Device encryption is required to resolve. Select the Home button, browse to Settings -> Security -> Encrypt Device / Phone.

Note: If you have a Samsung Galaxy S7 or S7 Edge, proceed to step 25.

20. If the battery is below 80% a warning will appear. Charge the phone over 80% and plug the phone up to a charger to proceed.

21. Select Encrypt Phone to proceed.
22. Enter the passcode

![Image of a passcode screen]

23. Select Encrypt Phone again to verify and begin

![Image of a passcode screen with a message]

24. Encryption could take a few minutes to an hour depending on the speed of the phone

25. By default the OS is encrypted, to complete encryption a startup PIN is required.
   a. Launch the Settings Application
   b. Scroll Down and Tap on the ‘Lock Screen and Security’ Option
   c. Then Tap on the ‘Protect Encrypted Data’ Option
   d. Tap on the ‘Require Lock Screen’ Option
   e. Tap on the ‘OK’ Button at the Bottom
   f. Input Your PIN to Confirm
   g. Then Reboot the Galaxy S7 to See it in Action

26. After Encryption is complete enter the passcode again to start the phone

![Image of a passcode screen]
27. From the Home screen select the company portal

Note: After downloading the icon displayed is “Company Portal” on the home screen

28. Select Devices and select the Android device with the exclamation point next to it

29. Select Check Compliance, this could take a few minutes

30. After the check completes, the device is now compliant. Return to the previous screen and select Apps
31. Select Outlook from the App Store

32. Select View in Google Play

33. Select Install from the store page

34. After downloading select Open to launch
35. Select Get Started on the wizard

36. Enter your health.slu.edu provided email address (example: joe.smith@health.slu.edu), select Continue

37. Select to Allow or Deny Access to contacts

38. Choose to add an additional email account or Skip to proceed (Skip was selected for the instructions. Additional accounts can be added later)
39. Select the arrow (selected for the instructions) or skip to proceed through the wizard

40. Select the arrow to proceed

41. Select the Check mark to complete the wizard

42. Select Ok to verify the data protection, this completes the installation and will launch Outlook to begin reading email
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>43.</strong> Once Outlook is installed, open the applications and select Settings in the upper right corner.</td>
<td><strong>44.</strong> Select the Office 365 Account</td>
</tr>
<tr>
<td><img src="image1.png" alt="Image" /></td>
<td><img src="image2.png" alt="Image" /></td>
</tr>
<tr>
<td><strong>45.</strong> Enable Sync Contacts</td>
<td><strong>46.</strong> Select Enable to start the Sync process.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td><strong>Sync contacts</strong></td>
</tr>
<tr>
<td>Automatic replies</td>
<td>1 Outlook contact will start syncing to your device.</td>
</tr>
<tr>
<td>Off</td>
<td>CANCEL ENABLE</td>
</tr>
<tr>
<td>Sync contacts</td>
<td></td>
</tr>
<tr>
<td>Advanced settings</td>
<td></td>
</tr>
</tbody>
</table>