Securing O365 with Workspace One UEM

Part 1: Configure Azure for Integration with Workspace ONE UEM

In this lab you will configure and apply data loss prevention (DLP) application policies to the Microsoft Intune App Protection applications and data in the Workspace ONE UEM console. Workspace ONE UEM does not directly enforce policies on applications. The Microsoft SDK controls and enforces the policies.

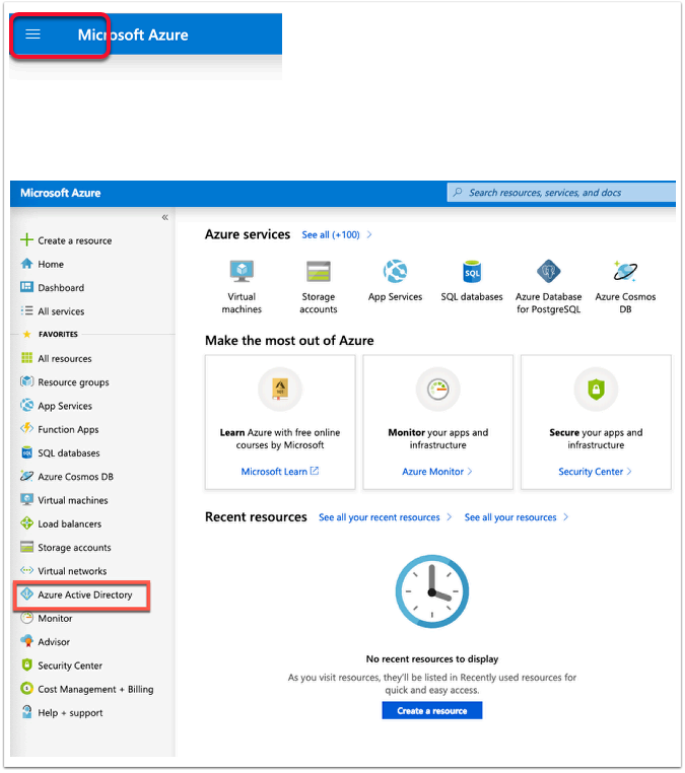
Pre-requisites:

1. Enterprise Mobility + Security E5 License (EM+S E5)

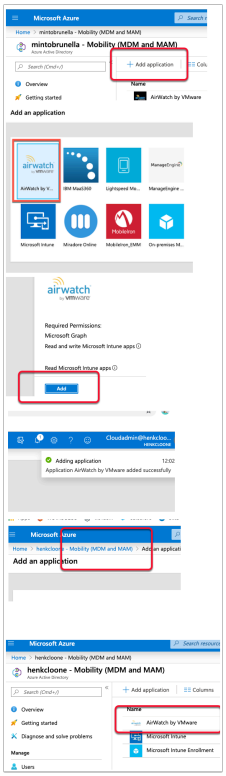
2. Admin credentials with access to Azure Active Directory with permissions to add enterprise applications and with the Group.Read.All and Group.ReadWrite.All permissions.

Note: Graph API does not support modern authentication. Hence can only use non federated Admin credential. Use *onmicrosoft.com domain.

1. Login to **portal.azure.com** using your onmicrosoft admin account created in an earlier lab.
    1. On the landing page select the ☰ 3 **horizontal lines** in the top-left hand corner to open the **admin menu**
    2. Select the **Azure Active Directory** from the left hand navigation pane.

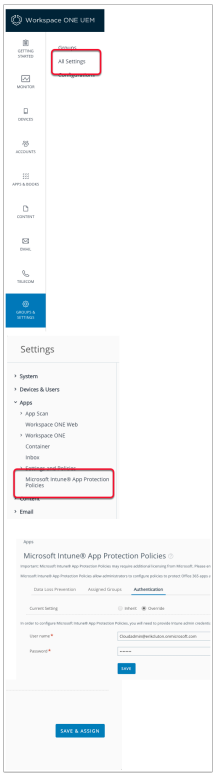


2. In the left pane select **Mobility (MDM and MAM)**
    1. In the **Mobility (MDM and MAM)** select **+ Add application**
    2. Select the **AirWatch by VMware** application, **scroll down** to the bottom right-hand corner
    3. Select **Add** on the side panel that pops-up.
        - You should notice a brief **Added application** message with a green tick next to it
    4. Go back to **Mobility (MDM and MAM)** by selecting the **Mobility (MDM and MAM)** at the top of the screen
        - Notice you now have an **AirWatch by VMware** Application

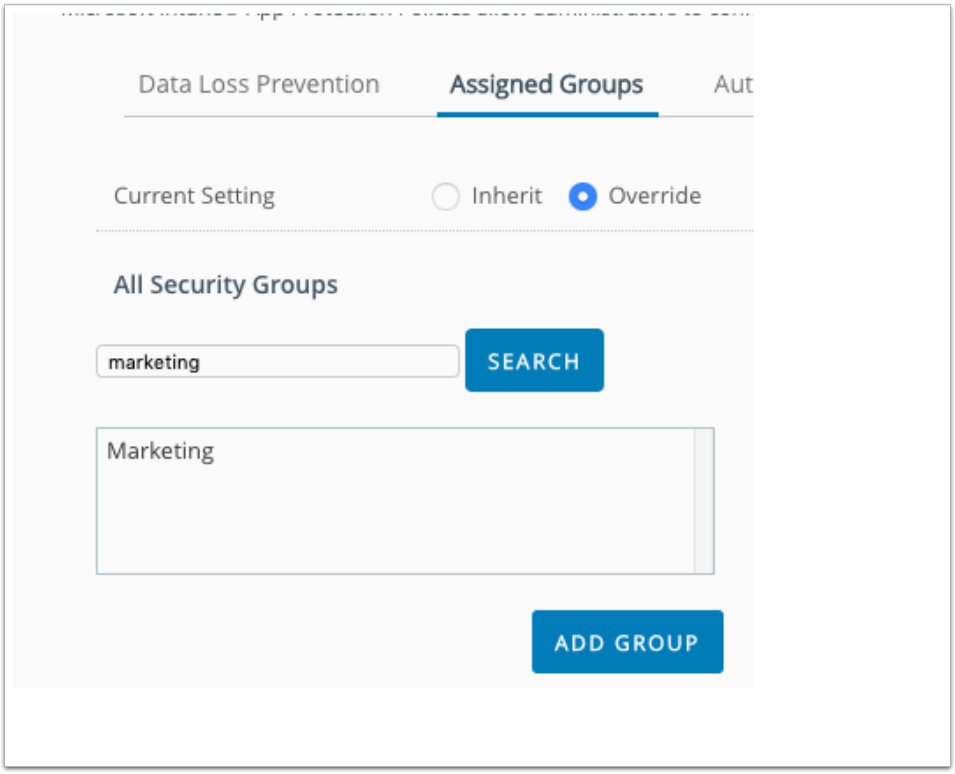


Part 2: Configure Workspace ONE UEM for Application Protection Policy

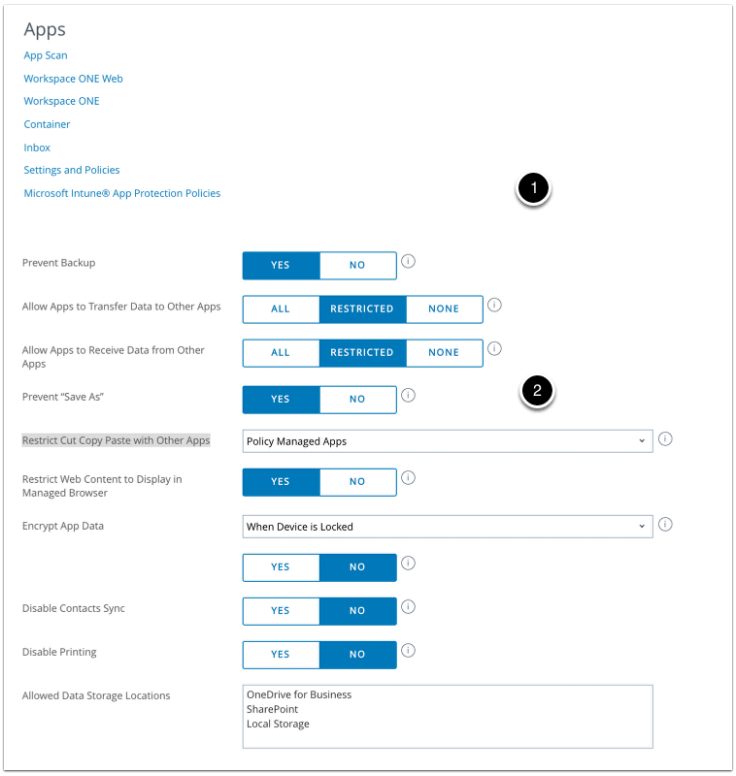
1. Configuring Data Loss Prevention using Microsoft Intune® App Protection Policies for Android and IOS Mobile devices
    1. Switch to your **Workspace ONE UEM** console and login as **Admin**
    2. Go to **GROUPS & SETTINGS** > **ALL SETTINGS**
    3. Under **APPS** , select **Microsoft Intune App Protection Policies**
    4. In the **Microsoft Intune App Protection Policies** console. Select the **Authentication** tab. Next to : -
        - **Username** : your **office 365 CloudAdmin username**
        - **Password** : your **cloud admin off365 password**
    5. Select **SAVE & ASSIGN**



2. In the **Microsoft Intune App Protection Policies** console
    1. Next to the **Authentication** tab to the left, select the **Assigned Groups** Tab
    2. Under **All Security Groups** select **SEARCH** Marketing
    3. Select **Marketing** select **ADD GROUP**
    4. Close the window by selecting the **X** in the top right-hand corner.



3. Ensure you are still logged into your **Workspace ONE UEM** admin console
    1. Select **GROUPs & SETTINGS** > **All Settings**
    2. In the **Apps Section** select **Microsoft Intune® App Protection Policies**
    3. Select the **Data `Loss Protection** tab, under **Data Relocation** section configure the following:-
        - **Allow Apps to Transfer Data to Other Apps : RESTRICTED**
        - **Allow Apps to Receive Data from Other Apps : RESTRICTED**
        - **Restrict Cut Copy Paste with Other Apps : Policy Managed Apps**
    4. Select **SAVE & ASSIGN**



For Intune Policies to be applied on **Android devices** we have to install the **Microsoft Intune company Portal app.**

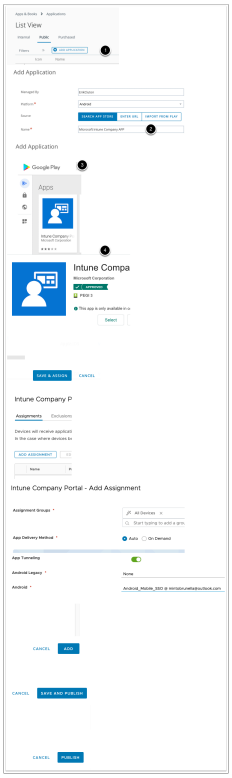
Part 2.1: Installing the Microsoft Intune Company Portal App (Android Only)

In the**APPS & BOOKS**>**Applications**>**Native**>**Public**tab

1. Select **+ADD APPLICATION**
2. In the **Add Application**window next to: Select
    - **Platform***: **Android**
    - **Name*: Microsoft Intune Company Portal App**

- select **NEXT**

3. In the **Add Application** window select **Intune Company Portal**
4. In the **Intune Company Portal** section, click the **Select** button
5. Select **SAVE & ASSIGN**
6. On the **Intune Company Portal- Update Assignment** window select **ADD ASSIGNMENT**
7. In the **Intune Company Portal- Add Assignment** window next to:-
   - **Select Assignment Groups: All Devices**
   - **App Delivery Method: AUTO** radio button
   - **App Tunneling :** ENABLED (notice two extra lines are added)
     - **Android*** Android_Mobile_SSO
8. At the bottom of the page select **ADD**
9. Select **SAVE & PUBLISH**
10. Select **PUBLISH**



Part 3: Test App Protection Policies

Now that the settings have been setup in the Workspace ONE UEM console, we must actually see these policies in effect on the device to enhanced security.

Wait 5 to 10 minutes for those policies to be applied to your device.

Part 3: Is divided into 2 sections

Section 1 : We test with an IOS device

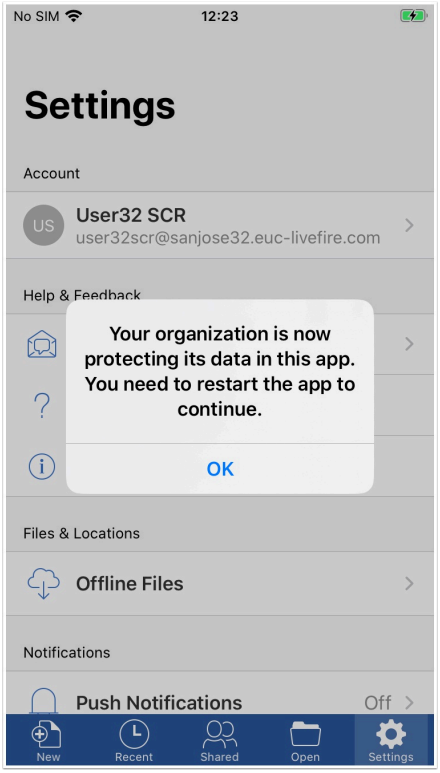
Section 2 : We test using an Android device

If you have not done any IOS configuration move on to Section 2 in Part 3 of this Lab.

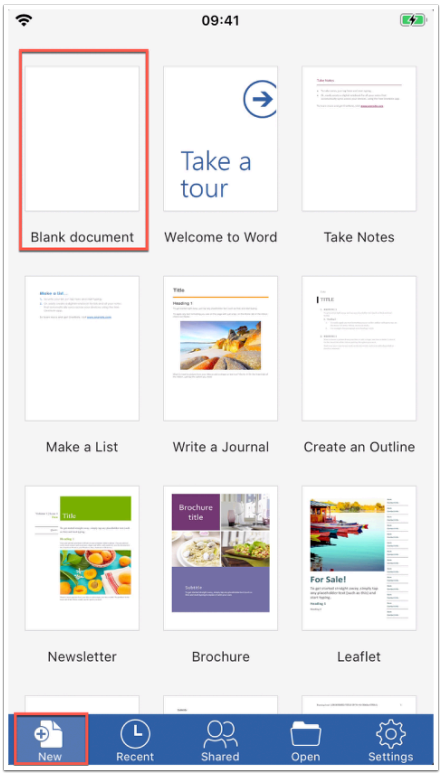
Section 1: IOS TEST

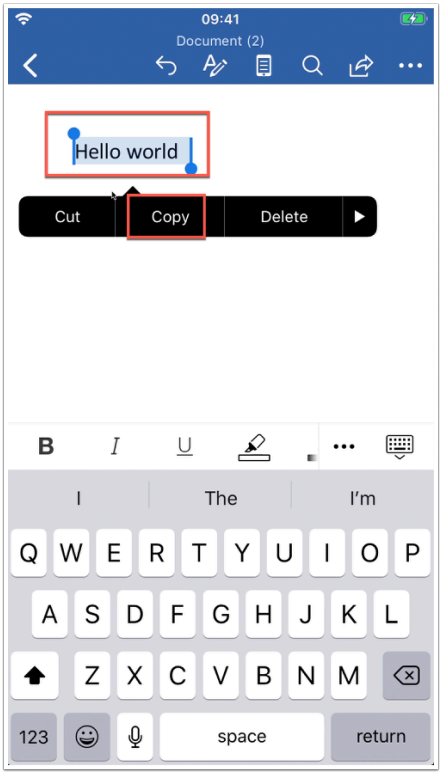
Note: The following steps have been written assuming you have NO previously installed Native Office 365 Applications on your IOS device prior to enrolling your device. If you suspect you have, for consistent results, that are in line with the instructions in this Lab, remove these native applications, and install Microsoft Word and Microsoft Excel through the Workspace ONE HUB application.

1. Ensure your IOS device is enrolled your lab environment and all previous parts of these labs have been completed successfully
    1. On your **IOS** device launch **Microsoft Word**
        - You will now see a prompt that the application has received additional Company Policies, select **OK** to close the window
    2. You will be prompted to set a passcode in accordance with the policy. Set a **4 digit pin** e.g. **2019**

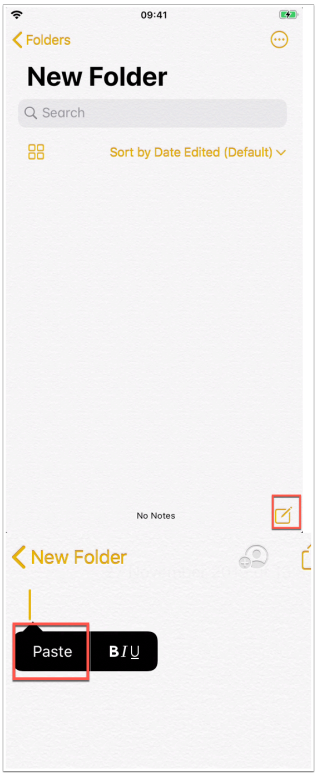


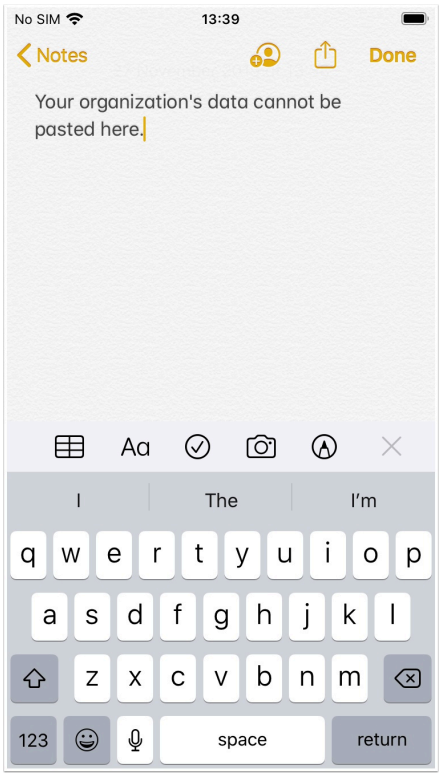
2. Let's now look at the Data Loss Prevention feature.
    1. In the **Word app** on your iOS device click on **New** at the bottom left to create a new document.
    2. Click on **Blank Document** in the top left corner.
    3. Now type **Hello World**, then **select** and click **copy**
    4. Now open **Notes** as an application on the device
    5. Click the **Pen on paper icon** in the bottom right corner of the application for a new note.
    6. Now **press and hold** to select **Paste.** You will get a message saying **"Your Organisation's data cannot be pasted here.**"


09:41
Blank document
Take a tour
Welcome to Word
Take Notes
Make a List
Write a Journal
Create an Outline
Newsletter
Brochure
Leaflet
New
Recent
Shared
Open
Settings


09:41
Document (2)
Hello world
Cut
Copy
Delete
I
The
I'm
space
return

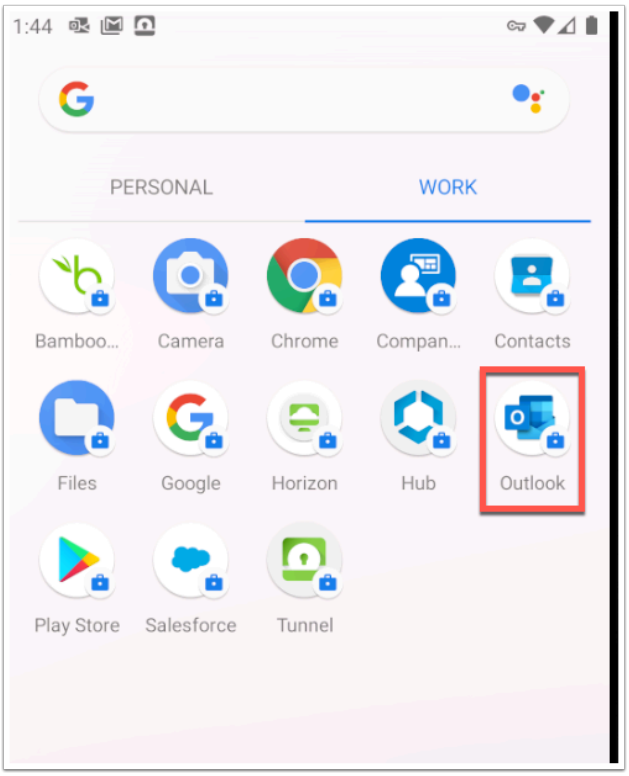

FaceTime
Wednesday
27
Calendar
Photos
Camera
Mail
Clock
Maps
Weather
Notes
Reminders
Stocks
News
iTunes Store
App Store
Books
Health
Home
Wallet
Settings
1

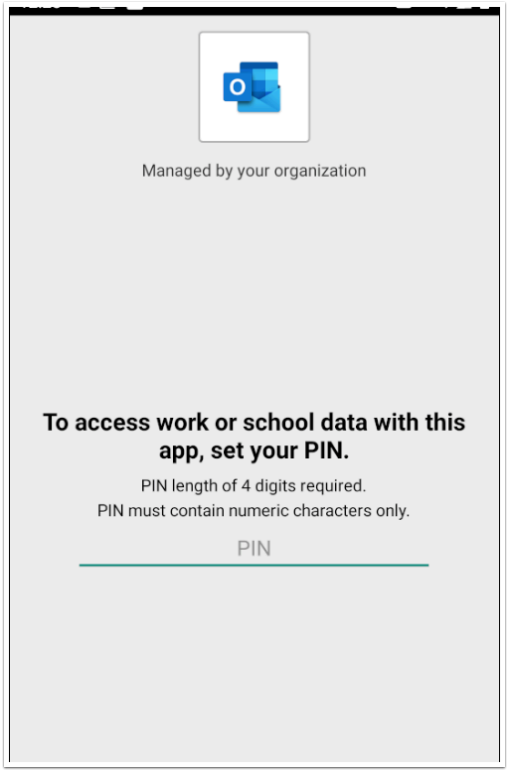

09:41
Folders
New Folder
Search
Sort by Date Edited (Default)
No Notes
New Folder
Paste
B I U

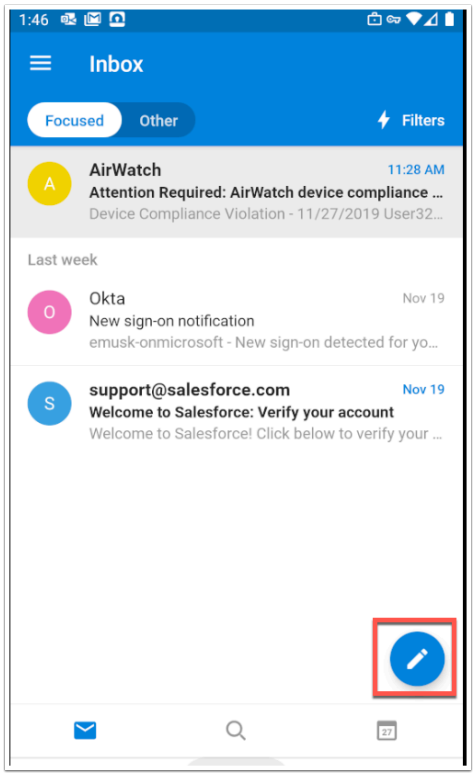


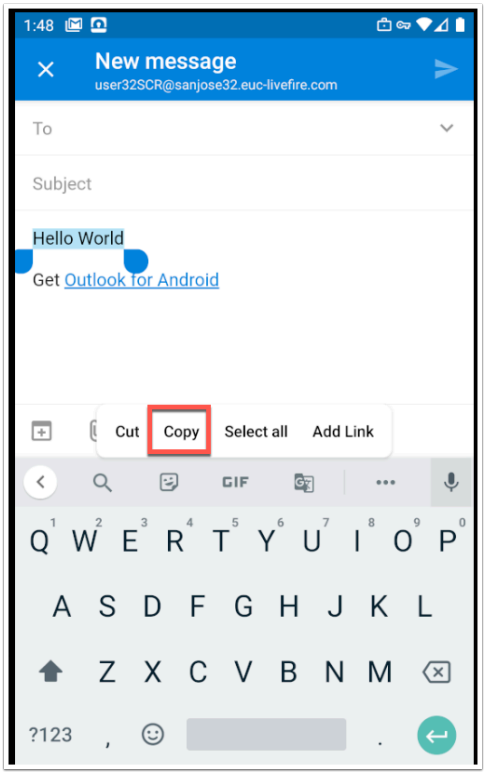
Section 2: Android OS Test

1. Ensure your Android device is enrolled your lab environment and all previous parts of these labs have been completed successfully.
    1. On your Android Device. Open the managed **Outlook** application
        - Notice the application is managed by your organization and you will be required to set a pin. Type **2019** or any four digit pin.
    2. Once you are in the **Outlook** application and you have entered the pin to authenticate, click on the **pencil icon** in the bottom right.
    3. Now in the body area of the new message type **Hello World**.
    4. **Select** the text and click **copy**


1:44
PERSONAL
WORK
Bamboo...
Camera
Chrome
Compan...
Contacts
Files
Google
Horizon
Hub
Outlook
Play Store
Salesforce
Tunnel


Managed by your organization
To access work or school data with this app, set your PIN.
PIN length of 4 digits required.
PIN must contain numeric characters only.
PIN





2. Now click **home** and click on the **Chrome** application that does not have the suitcase.
    1. In the **Chrome application** click on the address bar and click **Paste**
    2. You will note that it will not paste this text from Outlook. You will get a message "**Your organisation's data cannot be pasted here."**

- This concludes the Securing O365 with Workspace ONE UEM - you have seen the integration with Microsoft securing the digital workplace.