

## Navigating the Self-Self Portal (Android Devices)

### Logging into the Self-Service Portal (SSP)

1. Open the link below to access the Self-Service Portal:  
<https://airwatch.cuit.columbia.edu/MyDevice>
2. Make sure that the login method is set to “Email”
3. Type in your full Columbia **UNI** email address (ex: uni@columbia.edu) then click **Next**
4. At the next window enter your **UNI** (without @columbia.edu) and your **UNI password** and click **Log In**

The image displays two sequential screenshots of the Columbia Workspace ONE login interface. The first screenshot shows the initial login screen with the following elements: the Columbia Workspace ONE logo, a 'Select Language' dropdown menu set to 'English (United States)', a 'Login Method' dropdown menu with 'Email' selected (circled in red with a '2.' next to it), an 'Email Address' text field containing 'yourUNI@columbia.edu' (circled in red with a '3.' next to it), and a blue 'Next' button (circled in red). The second screenshot shows the subsequent login screen with the following elements: the Columbia Workspace ONE logo, a 'Select Language' dropdown menu set to 'English (United States)', a 'Username' text field containing 'UNI' (circled in red with a '4.' next to it), a 'Password' text field with masked characters (circled in red with a '4.' next to it), a blue 'Log In' button (circled in red), and a link for 'Trouble logging in'.

## Performing Remote Actions for Enrolled Android Devices:

5. After you have logged into the portal you will see a list of your enrolled devices on the header of the page. First choose your current device from the toolbar above
6. The SSP offers basic remote actions that can be performed on your managed Android device. Below are some of the **Basic Actions** you can perform in the portal:
  - a. **Change Passcode:** Change the current unlock passcode of this device.
    - i. You will be prompted to enter your new unlock passcode

Change Device Passcode

Password\*   Show Characters

Confirm Password\*

This action forces a new device unlock password on the user. The given password must be compliant with the current installed passcode policy constraints except for passcode history. If it does not meet these constraints, then it will be rejected

- b. **Lock Device:** Remotely locks device and offers the option to leave a custom message and callback number on the lock screen
    - c. **Device Query:** Sends updated device information to the CUIT managed console
    - d. **Sync Device:** Sends updated company settings and data to device
7. Currently there aren't any **Advanced Actions** that are available for users
8. To check your device's details click the **Go to Details** button next to Enrollment Status

My Devices

5. rp2706 Android Android 12.0.0 468Y  
Enrolled

rp2706 iPhone iOS 15.3...  
Enrolled

rp2706 Android Android 12.0.0 468Y

ENROLLMENT DATE 4/11/2022 4:07 PM

LAST SEEN 4/11/2022 4:16 PM

STATUS **1** Issue needs to be addressed

8. Go to Details

BASIC ACTIONS | ADVANCED ACTIONS

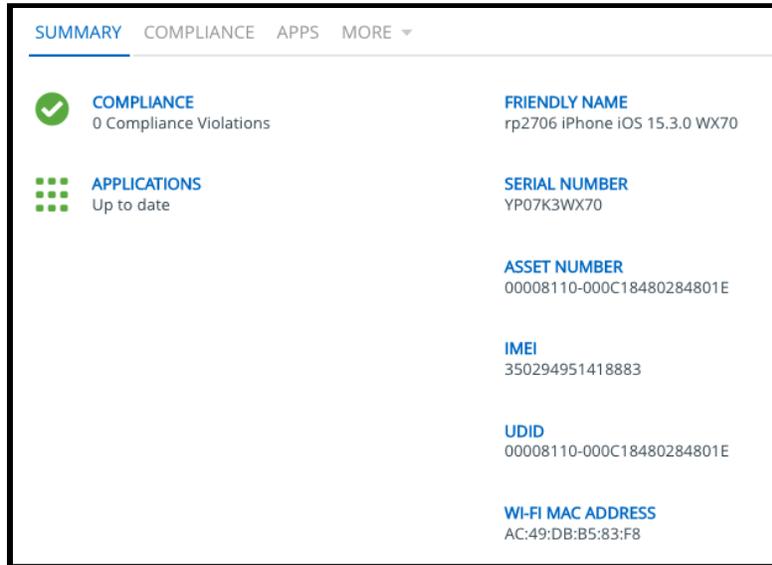
**6a.** Sync Device  
Send updated company settings and data to this device.

Lock Device  
Remotely lock this device to protect data.

Change Passcode  
Set a new passcode for this device.

## Checking Device Details Page:

1. At the next window you will first see the **Summary** tab which provides a quick overview of device details.



The screenshot shows the 'SUMMARY' tab of a mobile device management interface. The navigation bar at the top includes 'SUMMARY', 'COMPLIANCE', 'APPS', and 'MORE'. The main content area is divided into two columns. The left column contains two sections: 'COMPLIANCE' with a green checkmark icon and '0 Compliance Violations', and 'APPLICATIONS' with a green grid icon and 'Up to date'. The right column lists device identifiers: 'FRIENDLY NAME' (rp2706 iPhone iOS 15.3.0 WX70), 'SERIAL NUMBER' (YP07K3WX70), 'ASSET NUMBER' (00008110-000C18480284801E), 'IMEI' (350294951418883), 'UDID' (00008110-000C18480284801E), and 'WI-FI MAC ADDRESS' (AC:49:DB:B5:83:F8).

2. Clicking the **Compliance** tab shows if your device is currently compliant with Columbia's management policies.



The screenshot shows the 'COMPLIANCE' tab of the mobile device management interface. The navigation bar at the top includes 'SUMMARY', 'COMPLIANCE', 'APPS', and 'MORE'. Below the navigation bar is a table with three columns: 'Status', 'Policy Name', and 'Last Compliance Check'. The table contains one row with the following data: 'Compliant' (with a green checkmark icon), 'Compromised Status', and '3/21/2022 5:00 PM EST'.

Status	Policy Name	Last Compliance Check
Compliant	Compromised Status	3/21/2022 5:00 PM EST

3. Clicking the **Apps** tab shows work-managed applications installed on a device

SUMMARY COMPLIANCE **APPS** MORE ▾

Last Application Scan : 3/21/2022 5:00:23 PM

Name	App Status
Hub	Installed (22.02.0)

4. Click **More** and then click **Security** to view device security information

SUMMARY COMPLIANCE APPS **SECURITY** ▾

**Hardware**

- ✓ Is Not Compromised

**Encryption**

- ✓ Data protection is enabled.
- ✓ Block level encryption is enabled.
- ✓ File level encryption is enabled.

**Network**

- ✓ SIM Card Status Normal

**Profiles**

- ✓ All assigned profiles are installed.

**MDM**

- ✓ Enrolled

**Passcode**

- ✓ Passcode is present.
- ✓ Passcode is compliant.
- ✓ Passcode is compliant with profiles.

**Certificates**

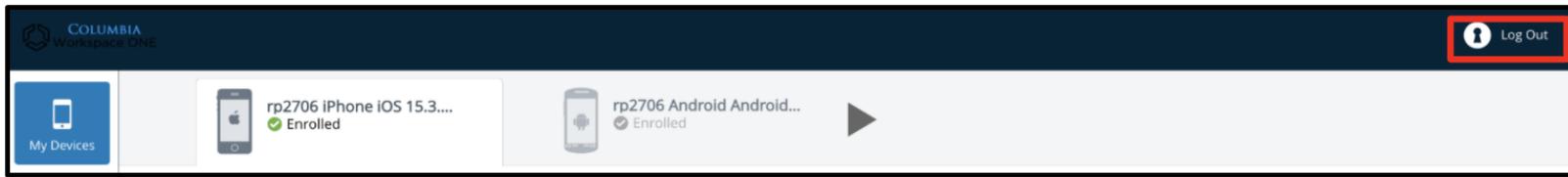
- 6 Certificate(s) currently installed.
- ⚠ Number of expiring certificates in 30 days unknown.

**Applications**

- 3 Active application(s).

## CUIT Support Contact & Logging out:

1. Click the **Log Out** button on the top right corner of the page



2. Please note the contact information for CUIT's helpdesk listed on the bottom left corner of the page. For technical questions or assistance, please submit a ticket to the CUIT Service Desk, email [askcuit@columbia.edu](mailto:askcuit@columbia.edu) or call 212-854-1919

