What is AirWatch?

AirWatch is a Mobile Device Management (MDM) service that will allow us to provide better security for smartphones, tablets and most mobile devices that will connect to the WUSM-Secure WiFi network. Airwatch has been selected as the enterprise solution to manage mobile devices. It will allow WUSM to provide better security for smartphones, tablets and most mobile devices using a mobile operating system that will connect to the WUSM-Secure WiFi network. In addition, AirWatch will help WUSM comply with federal and state regulations. The Encryption Subcommittee chaired by the FPP Board recommended an enterprise solution to provide consistent and timely reporting for compliance.

Why do we need the AirWatch service?

As mobile devices become increasingly powerful tools, so does their use in the work-place. As the differences between a mobile device and a traditional computer begin to dwindle we have to start thinking of them in the same way from a security standpoint. This means taking steps necessary to protect our devices and minimize the chances of a data breach, in the same way we would do that on a computer. This is what the AirWatch service will allow us to do.

Why do I now need an App to connect to the wireless network on campus? I didn’t need one before and I don’t need one when I am at home.

All mobile devices connecting to the WUSM-Secure WiFi network will now require the installation of the “AirWatch MDM Agent” App. As with most things you do on your device, an App is required. This App is free, and allows your mobile device and the AirWatch service to integrate closely with the existing university network, to better ensure that the only person who can access your email and data will be you.

Will this require that I have a passcode on my device?

Yes, pin and encryption are required. You may already have this from connecting to WUSM e-mail. The system will recognize the same pin you used before.

I already have a password on my device, so why is this App and the service needed?

Airwatch enhances our ability to work with mobile OS devices, e.g. iOS, Android, Windows phones. If a device is lost or stolen, a data wipe can be sent to the device thereby securing (removing) any sensitive data that may reside on it. Airwatch allows for a wipe of WUSM data pushed to the phone by Airwatch or a full factory wipe of the device.
Do I need to back up my device prior to installing AirWatch?

Airwatch will enforce pin and encryption on the mobile device. We recommend backing up your device (to separate system, not the Sim card) prior to encrypting your mobile device.

Will the AirWatch MDM Agent affect the battery life of my device?

On Android and Apple iOS devices, the AirWatch service primarily communicates to your device by the “push notification service”. This is also how your mobile device receives SMS messages, new emails, and voicemail notifications. The benefit of this is that the AirWatch MDM Agent is not constantly talking to the AirWatch service, and draining your battery while it does so. Any effect on the life of your battery will be negligible. If you are experiencing a noticeable decline in your battery’s performance after the installation of the AirWatch MDM Agent, please contact your support helpdesk so the issue can be addressed.

Will the AirWatch MDM Agent use my data plan?

The app will use a minimal amount of data. In our testing we noticed between 6 MB – 30 MB.

Will my IT Department now provide phone support for me?

Airwatch will not change the support model for mobile devices or phones. Any questions should be addressed with the department’s IT group.

Is it going to interact with other Apps or cause things to crash?

The AirWatch MDM Agent should not interfere with any existing applications on your mobile device, or otherwise adversely affect your devices performance. The AirWatch service does have the ability to remove from the device university specific information, such login information and email data associated with said login information, in the event the device is lost or stolen.

I often disable unimportant apps on my phone to save battery and keep my mobile device from running slow. Is this AirWatch MDM Agent setup so that it can’t be shut off?

The AirWatch service requires the AirWatch MDM Agent to be installed and running on your device. Even though you shouldn’t be able to disable the AirWatch MDM Agent on your mobile device, behavior may differ from device to device. If the AirWatch MDM Agent does end up being disabled on your mobile device, the AirWatch service will no longer be able to verify that your device is allowed access to
the WUSM-Secure WiFi network. This would result in restricted access to the network from that mobile device, until the AirWatch MDM Agent is re-enabled on the device.

**When I am off campus, am I going to lose access to my work email on my mobile device?**

No. As long as you have good wireless connection, you should be able to access email on your mobile device exactly as you are able to now.

**If I am off campus, am I going to keep getting an annoying message about not being connected?**

No. After you are properly enrolled with the AirWatch service, it works behind the scenes and should be invisible.

**What happens if I turn off my phone and forget my password?**

While the AirWatch service will be able to help enforce this policy, there is no way to recover a forgotten passcode from a locked device.

**If someone steals my phone while it’s logged in, or they figured out my password, how will you be able to stop them from connecting as me?**

If your device and password are compromised, report it immediately. We can use the AirWatch service to remove any university related data and prevent it from reconnecting to the network.

**If I upgrade to a new phone do I have to have IT set up this App again, or can I do it myself?**

Yes, you will have to download and install the App on your new device. A setup guide will be made available to install the AirWatch MDM Agent and enroll your new device into the AirWatch service. As always, your support helpdesk is here to serve you and will be able to assist you with enrolling your device into the AirWatch service.

**Is there going to be some kind of icon or notification letting me know if I am connected?**

No. After you are properly enrolled with the AirWatch service, it works behind the scenes and should be invisible. The only visual change will be the addition of the AirWatch MDM Agent App icon in your device’s App listing.

**Is this compatible with any device? Android, iPhone, Windows Phone, etc?**
The AirWatch service is compatible with most Android and Apple iOS devices. Other mobile operating systems such as Windows Phone and Blackberry are supported to a lesser degree, but should be adequate to comply with our current mobile security policies.

**Are you going to be able to use this to access everything on my phone?**

Absolutely not! The AirWatch service is not spy-ware. It is a tool to help both you and the university protect important or confidential data. It does not give us the capability access and view data on your mobile device. It does provide access to view the apps installed on your phone. This view is has been restricted to WUSM support staff. We are only using the profiles that allow us to ensure your device complies with existing Washington University policy, pin and encryption.

**Is this just a way to watch all of the emails I send and websites sites I visit?**

Absolutely not! The AirWatch service is not spy-ware. It is a tool to help both you and the university protect important and/or confidential data.

**Will this affect my laptop?**

Not at this time. The current enrollment process is for mobile devices and tablets with a mobile operating system that need to have access to WUCON through WUSM-Secure.

**When I update my mobile (OS) device will I need to install the app again?**

Yes. You will need to install the app and enroll with the new device. Until this is complete you will not be able to connect to WUSM-secure.