AHS Secure Email Update & Bring Your Own Device – FAQs

How can I access my AHS email?
There are two ways you can access your AHS email and calendar on your desk/laptop or mobile devices:
1. Outlook Web Portal: use your usual AHS email and password.
2. Outlook application on your phone/tablet, in combination with the access management software Workspace One (WSO), as part of a Bring Your Own Device (BYOD) software solution.

What is Bring Your Own Device (BYOD) at AHS?
We recognize many physicians do not have an AHS-issued device. BYOD is a voluntary program allowing physicians to use their personally owned mobile devices to securely access AHS information and apps. BYOD protects sensitive data in a secure enclave on the user's device using a program called Workspace ONE. In the future, similar access for your personal laptops/desktops will also be enabled.

Why are we talking about BYOD?
The Outlook Web Portal is an enhanced email portal, however certain email and calendar features are not available on the Outlook Web Portal. BYOD and Outlook together enable seamless access to your AHS email, including push notifications on your personal devices. BYOD enables the secure use of the fully featured applications on your devices. BYOD enables seamless access to other AHS applications now and in the future (e.g., Connect Care).

Why would I want to enrol in the BYOD program, and use Outlook instead of Webmail?
Workspace ONE with Outlook offers advanced mail and calendar functions. It works exactly the same whether you connect via an AHS network or an external network. With Webmail, the browser-based interface requires regular login each time it is accessed and lacks full integration with local device capabilities. With the BYOD program, Workspace ONE and Outlook together mitigate these concerns. It simplifies access to AHS applications on your device on any network.

Will I be able to use other email applications?
You will not be able to access AHS email using other applications. You will be able continue to use your other email applications for your non-AHS email. Alternatively, you can also migrate those other email services to Outlook if you wanted to keep one email program. Your non-AHS email would not be visible to AHS.

What is the AHS Workspace ONE platform?
AHS uses VMWare's Workspace ONE security software to provide Enterprise Mobility Management (EMM). Workspace ONE creates a protected space (called an enclave) where AHS applications (including business applications like email and clinical applications like Connect Care) run. In effect, it creates a trusted relationship between the user's mobile device and AHS while ensuring that the user maintains control over all applications and information outside of the enclave.

What effect will Workspace ONE have on my device?

Once installed, Workspace ONE only touches applications managed by Workspace ONE. Personal applications and their associated data are outside the Workspace ONE enclave.

Workspace ONE will not successfully install if a personal device does not meet College of Physicians and Surgeons of Alberta (CPSA) and AHS security requirements, including password protection and encryption.

Does Workspace ONE work on all platforms and versions?

Workspace ONE will be supported on the following platforms, as long as you have the current security updates:

- Apple iOS
- Android

In the future, Windows 10 and Mac OS laptops and desktops will be supported.

How is AHS-specific data stored using Workspace ONE?

AHS-specific data is stored on a secured enclave on your device; this stored information can be wiped remotely if needed (e.g., if the device is lost or stolen). **In this case, only AHS data will be removed.**

Will AHS be able to see all of the data (e.g., personal email or banking) on my device?

No, AHS will not gather any information about your movements or device usage outside of those apps managed through Workspace ONE. The sole purpose of mobility management is to guarantee the security of interfaces to the clinical information for which AHS is accountable, given that these may contain personal health data. AHS does not use mobility management to monitor any of your personal information or data on personal devices. For additional guides and information, please refer to Connect Care Mobility.

Will Workspace ONE force me to change any of my device settings?

In order to enrol your device into Workspace ONE and to maintain compliance, AHS must verify that your device is password protected and has been encrypted. AHS will not apply any other restrictions.

If I enrol in BYOD, can I still use a virtual private network (VPN) and my usual antivirus/antispam software?

As long as your VPN/antivirus software allows access to the public internet, Workspace ONE and AHS email through Outlook will not be interrupted. If you're not sure if this is the case for you, please contact your software provider.

Does Workspace ONE provide a VPN for my other applications?

Workspace ONE does not function as VPN for non-AHS applications.

I already have Outlook installed; do I need to reinstall using the AHS app portal?

Current versions of Outlook on supported mobile devices do not need to be reinstalled. These can be downloaded from the appropriate App stores on Android and iOS devices.

Will there be issues if I already use another Enterprise Mobility Management (EMM) solution (e.g., Workspace ONE through my academic institution)?

If your device is already enrolled with another organization's EMM solution, you will not be able to enrol your device into the AHS instance of Workspace ONE. You will still be able to access AHS email using the web application.

Can I publish my AHS calendar so anyone can subscribe to it?

With the transition to Microsoft O365, you will now have the ability to subscribe to your AHS calendar on any device or client. This function does not require Workspace ONE. For detailed instructions, please refer to Microsoft support documents for publishing a calendar.

Will this slow any applications on my device?

Any applications installed through Workspace ONE behave like any native piece of software. They will run as efficiently as any other application running on your device. Workspace ONE should not affect the performance of any of your other applications.

Will I need to enter passwords each time I use apps in EMM? Is there a timeout period?

Once you've set up Workspace One on your device and configured Microsoft Outlook, you will not be prompted to enter your AHS username and password to access your email (unless you choose to configure it otherwise). As a minimum-security requirement, you will need to enter your device password if the device has been idle for more than 10 minutes. Biometric unlocking, like a fingerprint scan can be used, if it is enabled.

Can I receive push email on mobile devices with EMM?

Yes. Using Microsoft Outlook desktop and mobile clients, you will be able to configure your notifications settings for your needs as per your device settings.

Do I have to enrol my personal device in BYOD if I already have an AHS-issued machine?

If you already have an AHS-issued device and it meets your needs, you do not need to enrol your personal device using the BYOD model.

Has this solution been validated by physicians?

Physician end user testing was conducted before roll-out, and instruction guides reflect the physician testing experience.

Where can I find more information?

- [Accessing AHS Email, Intranet and the Bring Your Own Device (BYOD) Program.](#)
- For technical issues, please contact the IT Service Desk at 1-877-311-4300.