BYOD/Hypori Microsoft Outlook Configuration with Encrypted Email (S/MIME)

Introduction

This document will instruct you how to complete set up the Microsoft Outlook Client application and how to configure digital Purebred certificates to enable encrypted email (S/MIME) in your Hypori Halo virtual workspace.

Prerequisites

To configure Outlook email, it is required that:

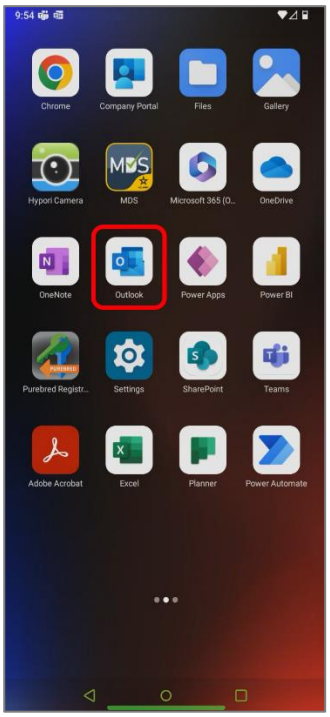
- Your Outlook email account matches the email address for the certificates on your CAC.
- You belong to an approved domain (e.g., army.mil, af.mil, etc.). For more information about confirming and/or correcting the naming of your CAC certificates, please contact AESD.
- Purebred certificates must be present on your Hypori Halo virtual workspace. Authentication to Exchange Online using Outlook Client and configuration of S/MIME require the Purebred PIV Authentication Certificate and the Purebred Digital Signature Certificate.
- BYOD/Hypori onboarding email containing the “BYOD.p12” file

Procedure

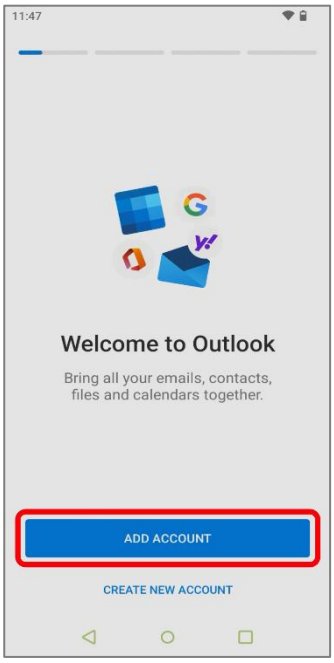
Outlook Client Setup with Encrypted Email (S/MIME)

Purebred certificates must be present on your Hypori Halo virtual workspace before continuing this procedure. Authentication to Exchange Online using Outlook Client and configuration of S/MIME require the Purebred PIV Authentication Certificate and the Purebred Digital Signature Certificate.

1. From the home screen of the Hypori Halo Client, open the *Outlook* app.

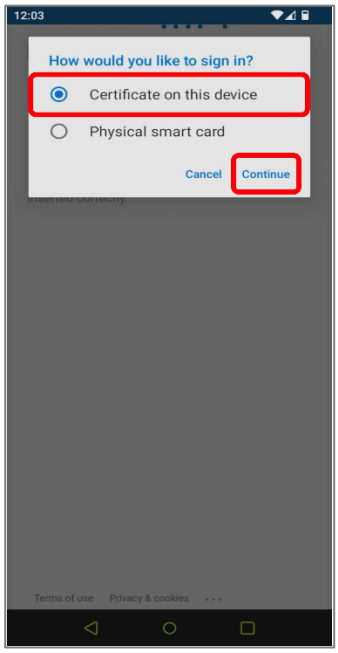


2. In Outlook, select *Add Account*.

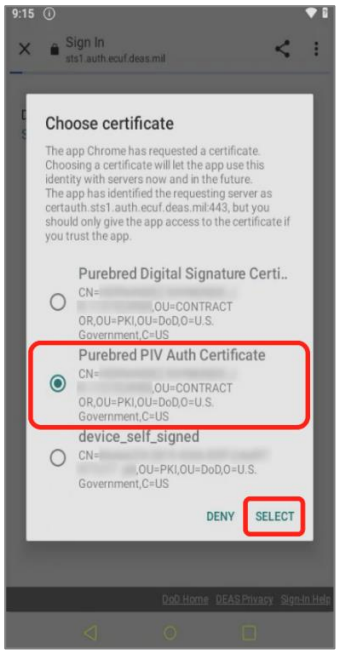


3. Enter or select your email address (e.g., username@army.mil), then select *Continue*.

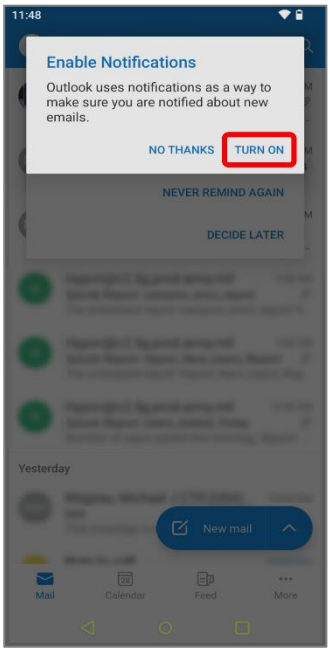
Note: The email address here must be a match to the address used for your CAC-based certificates and Purebred certificates.



4. When asked *How would you like to sign in,* choose *Certificate on this device*, then select *Continue*.

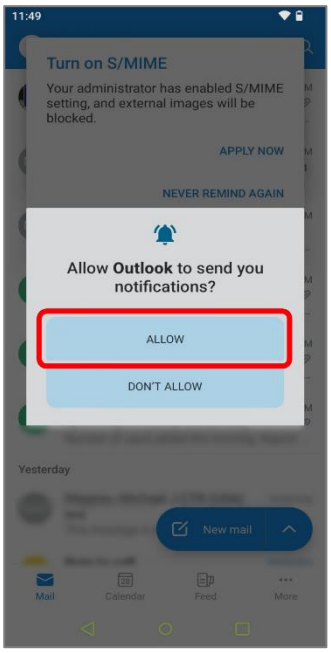


5. Choose the *Purebred PIV Auth Certificate*, then *Select.*

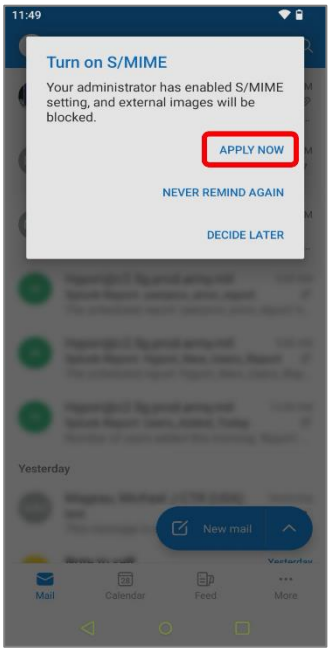


6. Select *Turn On* to enable Outlook notifications.

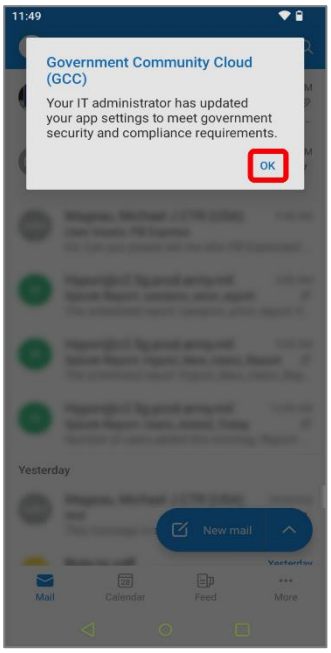
7. Select *Allow*.



8. Select *Apply Now* to turn on S/MIME.

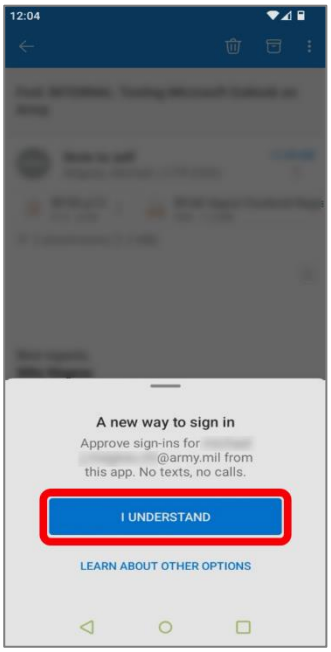


9. Select *OK* to dismiss the GCC acknowledgment.

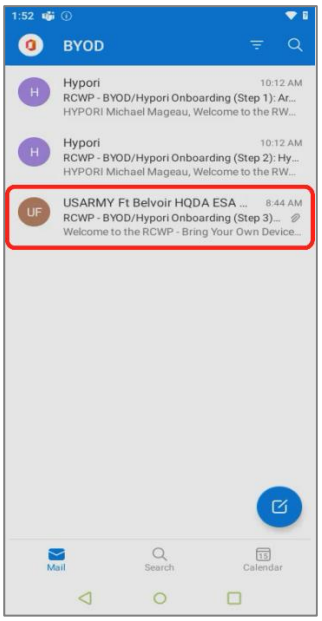


---

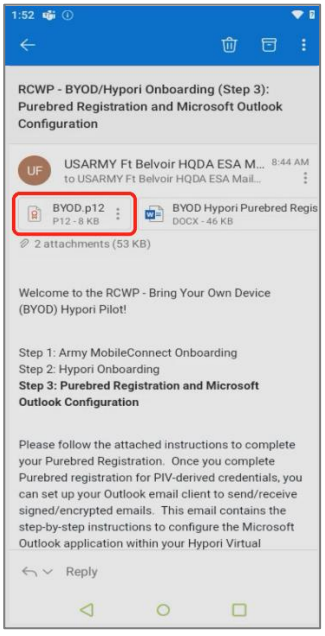
10. The first time configuring your account, you may be prompted for "A new way to sign in," Select *I Understand* to approve sign-ins.



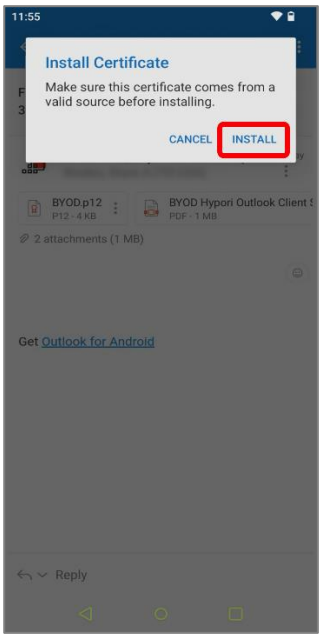
11. In your *Outlook* inbox, you will have received a BYOD/Hypori onboarding email. Open the email, which contains the PKCS #12 file as attachment (file extension .p12).



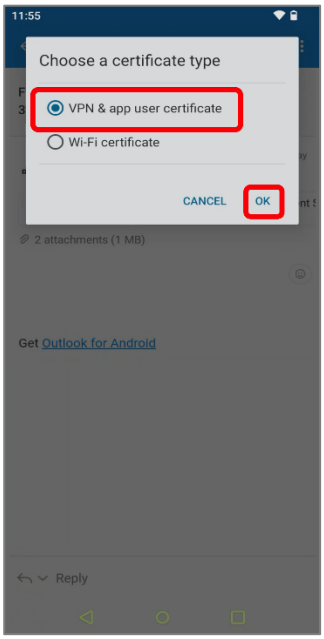
12. From the email, select and open the P12 attachment to begin the installation of your Purebred digital certificates.



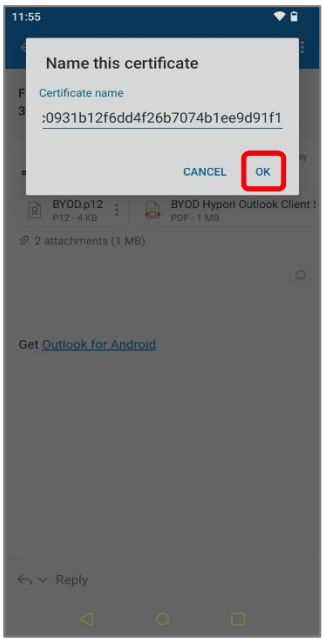
13. Select *Install*.



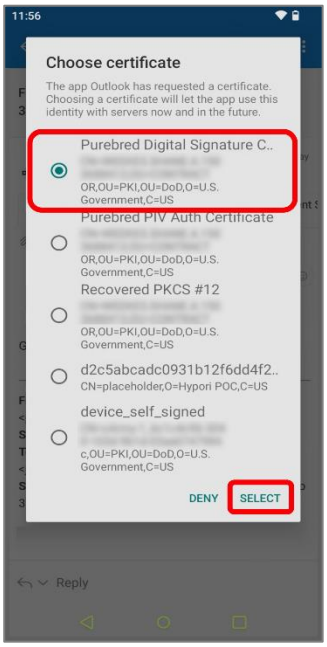
14. When prompted to *Choose a certificate type*, select *VPN & app user certificate*, then choose *OK*.

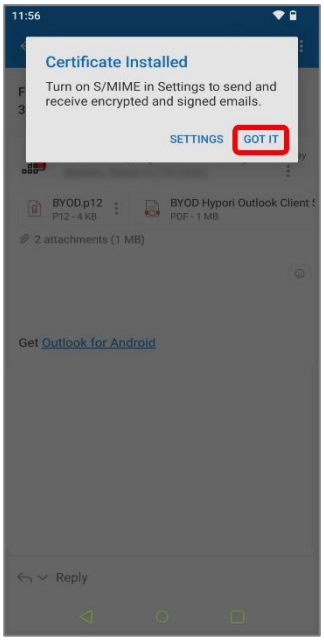


15. When prompted to *Name this certificate*, use the default certificate name. Select *OK*.

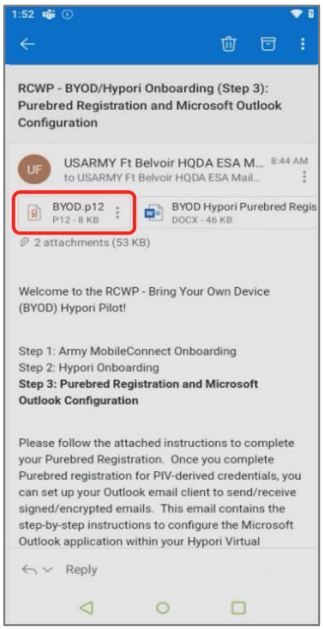


16. When prompted to *Choose certificate*, select the *Purebred Digital Signature Certificate*, then choose *Select*.



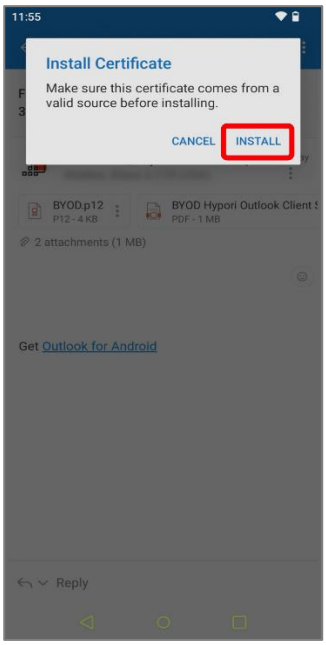


17. You will be notified that the *Certificate Installed*. While the message will instruct you to turn on S/MIME in Settings, you will complete this step later. Select *Got It*.

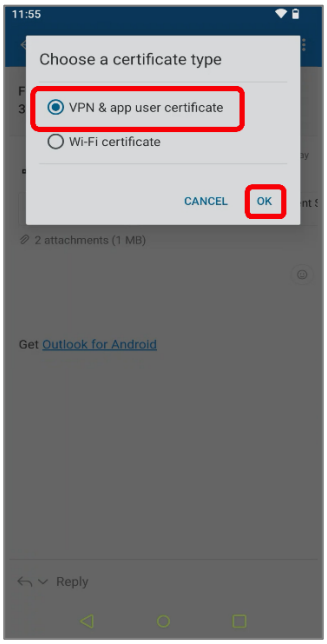


18. Next, install any recovered PKCS #12 certificates. Select the Hypori email's .p12 attachment to begin.

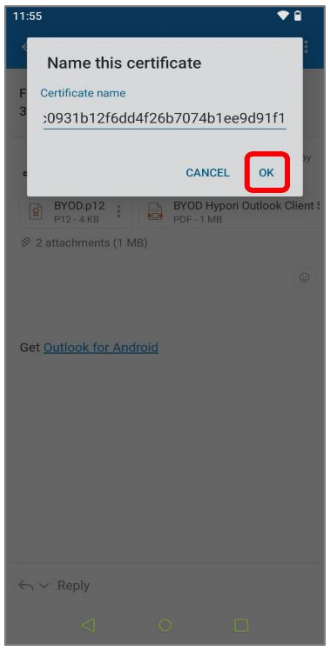
19. Select *Install*.



20. When prompted to *Choose a certificate type*, select *VPN & app user certificate*, then choose *OK*.



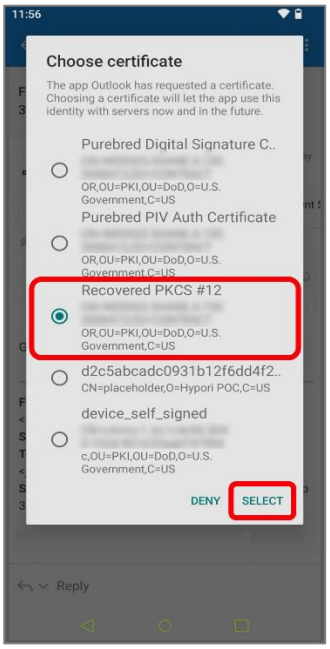
21. When prompted to *Name this certificate*, use the default Certificate name. Select *OK*.

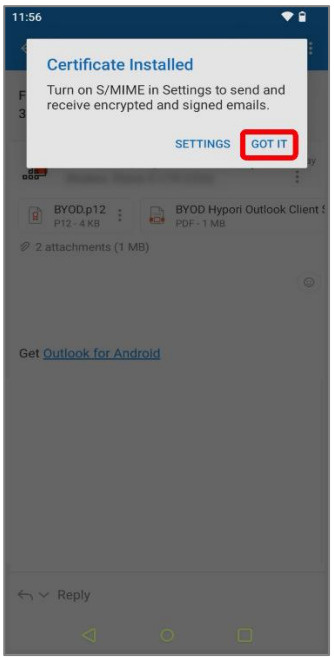


---

22. When prompted to *Choose certificate*, select the *Recovered PKCS #12*, then choose *Select*.

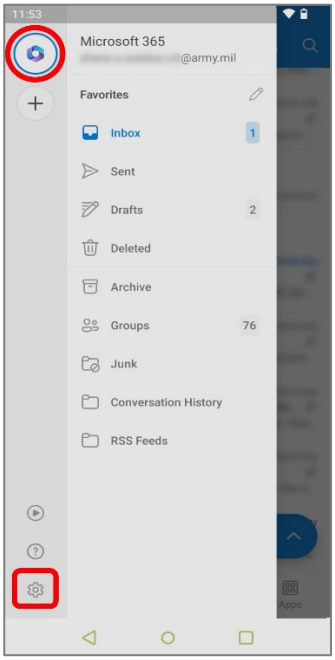
Note: If there is more than one Recovered PKCS #12 certificate here, take note because you'll have to complete this process for each one.





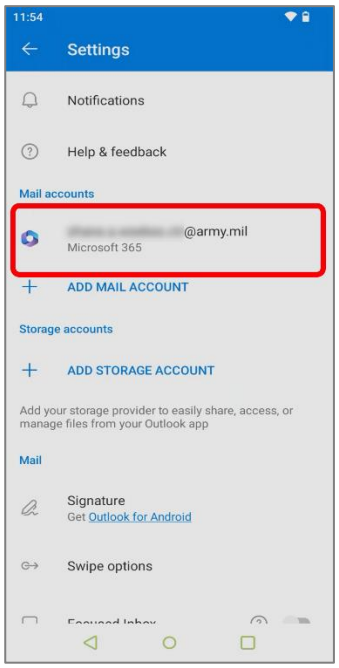
23. The *Certificate Installed* successfully.

a. If there are additional Recovered PKCS #12 certificates that must be added, select *Got It* and return to step 18.
b. If there are no additional Recovered PKCS #12 certificates that must be added, select *Settings* and continue to step 24.
c. After completion of certificate installation press the back arrow to close the email.

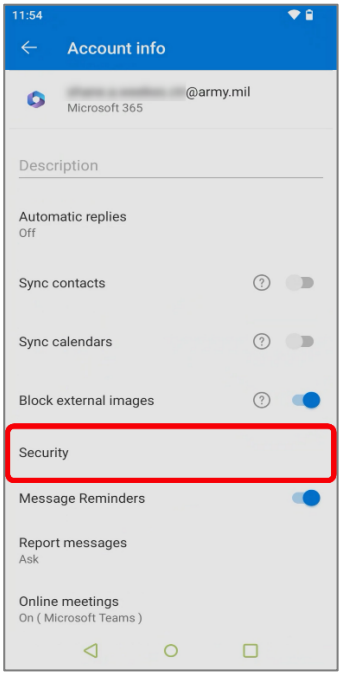


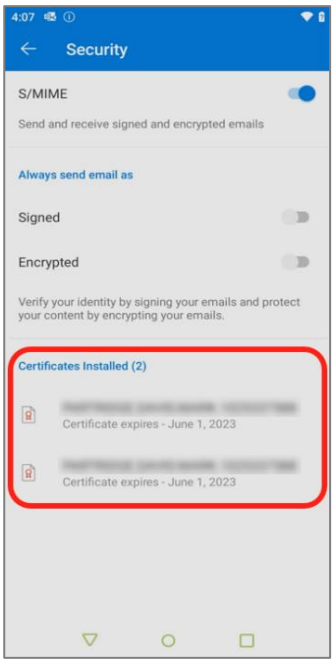
Note: The *Settings* menu can be accessed from Outlook by selecting the Office365 logo, then selecting the settings gear.

24. In the *Settings* menu, locate the *Mail accounts* section and select your account.



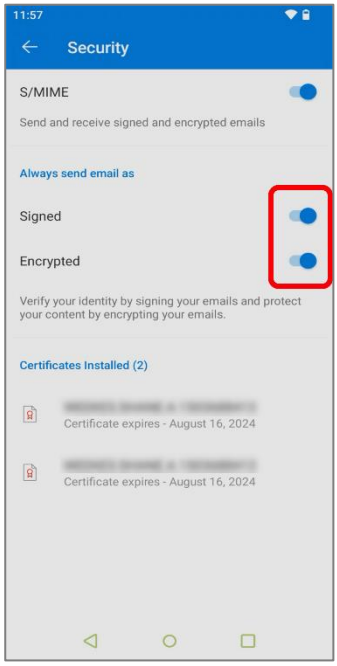
25. In the *Account info* menu, select *Security*.





26. In the Security menu, you can see *S/MIME* is enabled.
In the *Certificates Installed* section, you will see entries for the initial digital signature and for each recovered PKCS #12 certificate.

Note: If you receive an error when attempting to enable S/MIME, your Outlook account likely does not match the email address for certificates on your CAC. For more information about confirming and/or correcting the naming of your CAC certificates, please contact AESD.



27. Optional: In the Security menu *Always send email as* section:

- **a.** You can optionally select *Signed* to digitally sign your emails by default.
- **b.** You can optionally select *Encrypted* to encrypt your emails by default.

When these settings are enabled, each switch will slide to the right and turn blue.

Once complete tap the back arrow at the top of the screen three times to return to your inbox.