BYOD/Hypori New CAC Card: Purebred and Microsoft Outlook Reconfiguration

Introduction

When a user is issued a new CAC card, they must associate that new CAC card with their existing Hypori Halo Virtual Desktop by generating/loading new derived credentials using Purebred. This document will instruct you how to update your Purebred credentials if you receive a new CAC/PIV and how to configure those new digital Purebred certificates to enable encrypted email (S/MIME) in your Hypori Halo virtual workspace.

Prerequisites

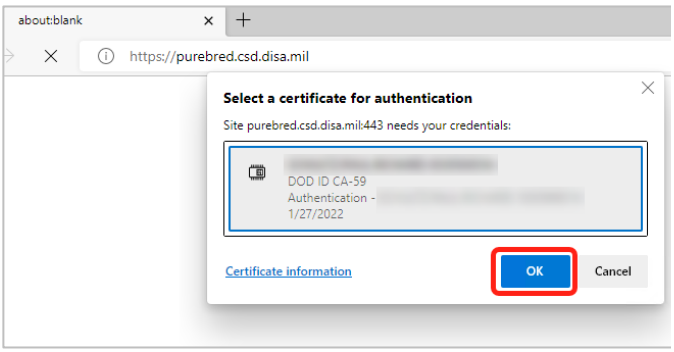
To complete the Purebred registration process, you must have Access to a NIPRNet-connected workstation.

To configure the Outlook email client and configuration of S/MIME, it is required that your new Purebred certificates must be present on your Hypori Halo virtual workspace. You will also need the BYOD/Hypori onboarding email containing the “BYOD.p12” file.

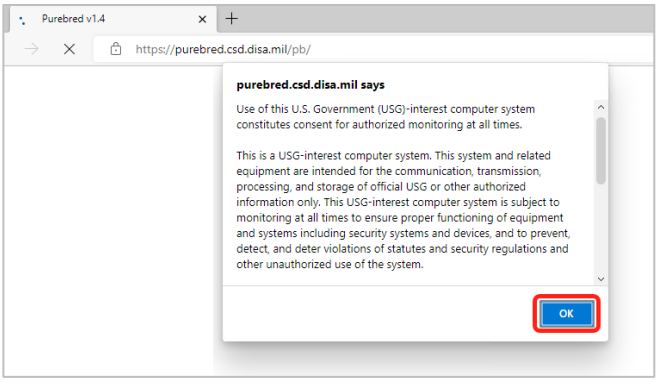
Procedures

New CAC Card: Generating New Purebred Credentials

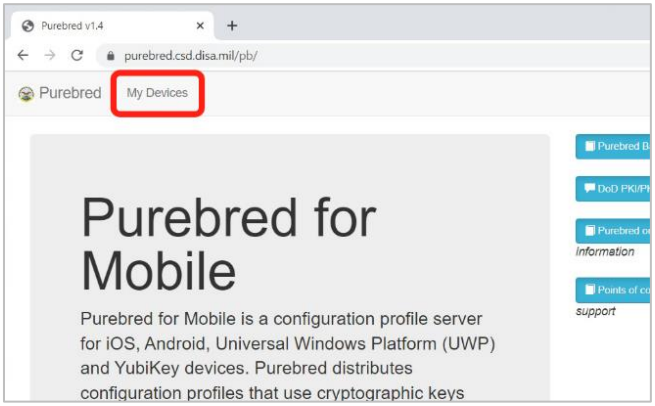
1. On a computer connected to NIPRNet, open a web browser and navigate to https://purebred.csd.disa.mil/. Select your PKI certs as requested.



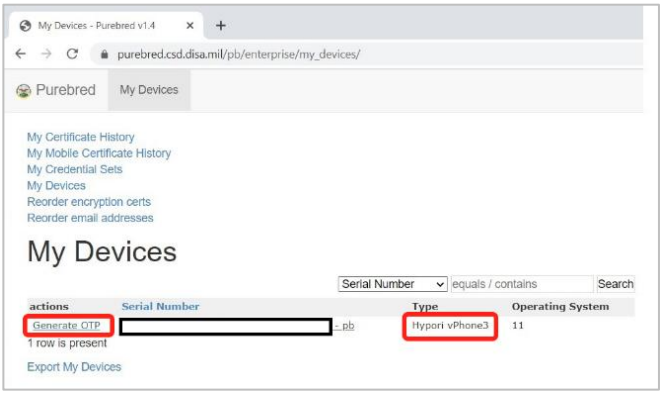
2. Select OK to accept the DoD Notice and Consent.



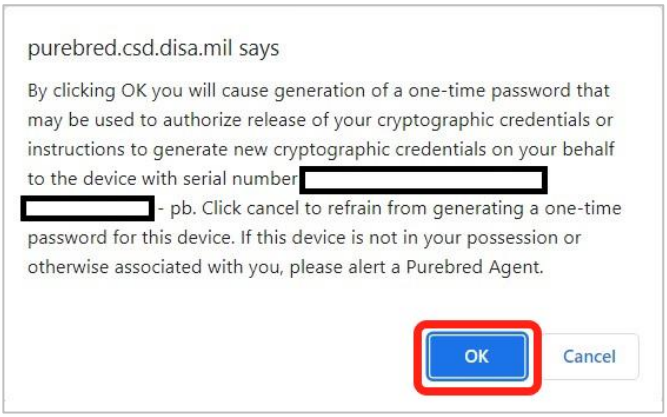
3. On the Purebred webpage, select *My Devices*.



4. On the *My Devices* webpage, there is a table containing information about the Hypori Halo virtual workspace, displayed here as *Hypori vPhone3*.
On this row, select *Generate OTP* from the actions column.

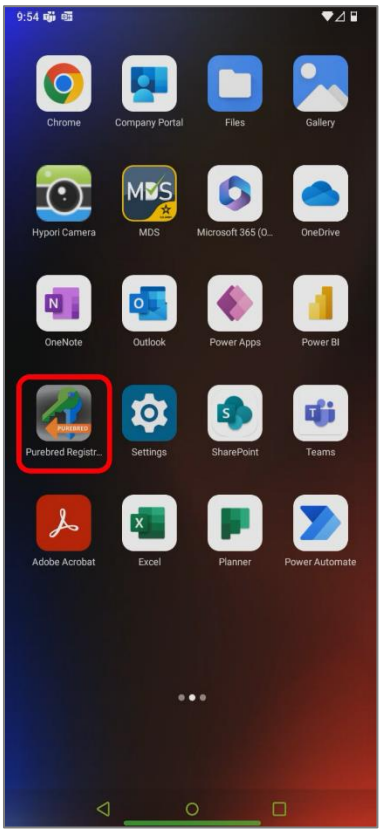


5. Review the security statement in the pop-up window, then select *OK*.

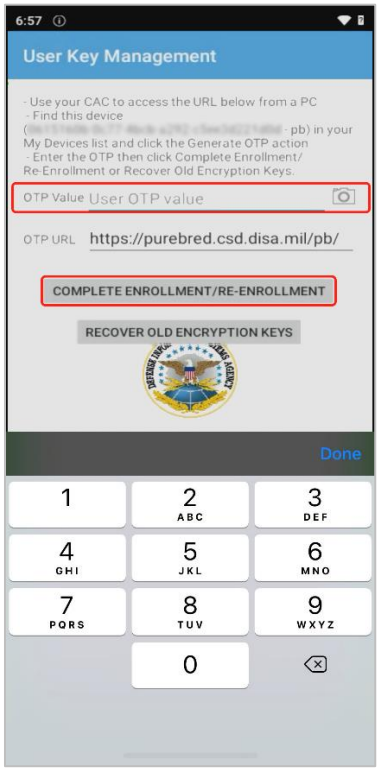


6. The webpage will return an 8-digit numeric one-time password (OTP). This OTP changes every three minutes; it is recommended to leave this page open so you can refer to it in later steps.
NOTE: QR Code is not supported at this time.

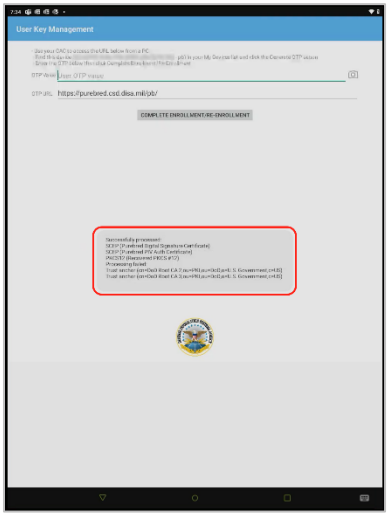
7. From your device, open the Hypori Halo Client app and select the Purebred Registration icon.



8. Once the Purebred app opens, enter the OTP from step 6 in the *OTP Value* field, then select *Complete Enrollment/Re-enrollment*.



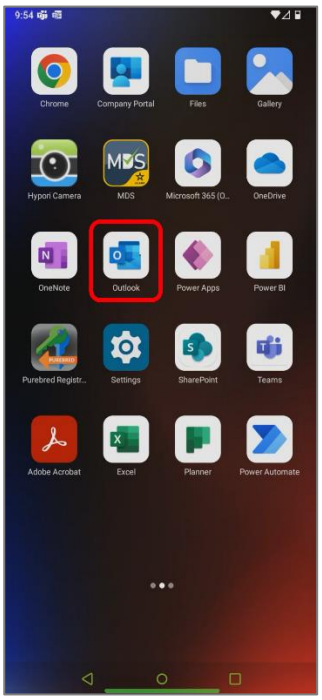
9. The derived credentials will begin downloading. You'll receive a Successfully Processed message once the process is complete.



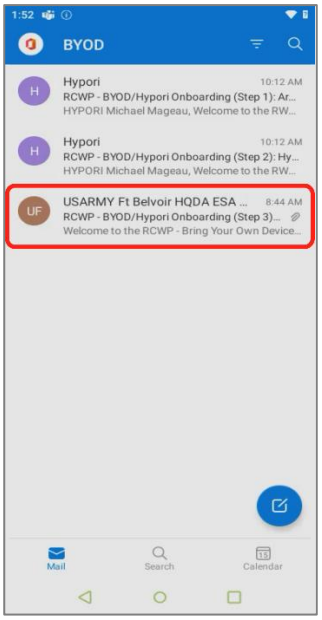
Outlook Client Setup with Encrypted Email (S/MIME)

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.

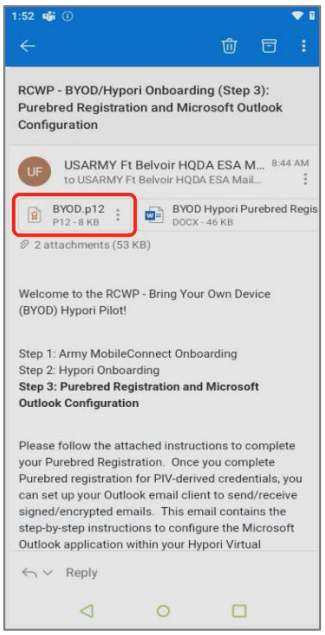
1. From the home screen of the Hypori Halo Client, open the *Outlook* app.



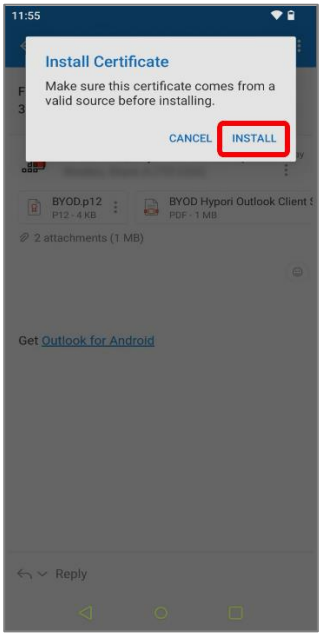
2. In your *Outlook* inbox, you will have received a BYOD/Hypori onboarding or transition to Outlook email. Open the email, which contains the PKCS #12 file as attachment (file extension .p12).



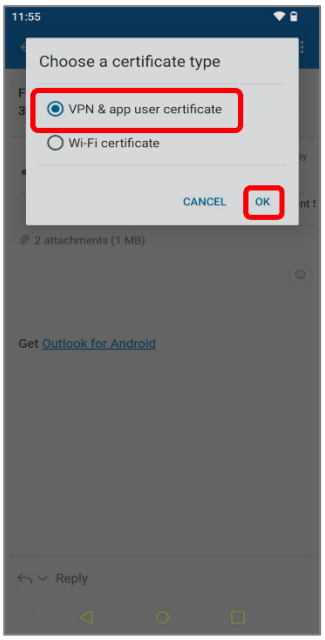
3. From the email, select and open the P12 attachment to begin the installation of your Purebred digital certificates.



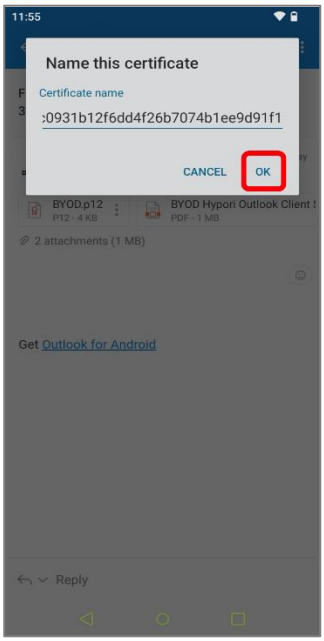
4. Select *Install*.

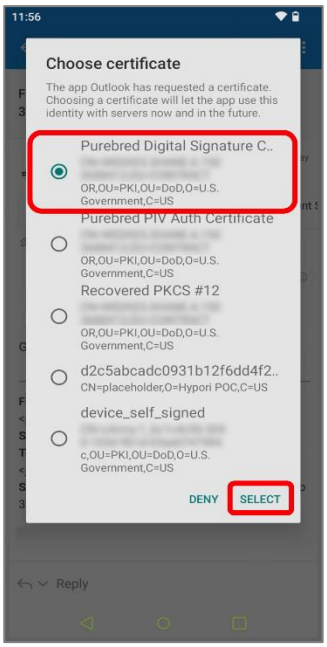


5. When prompted to *Choose a certificate type*, select *VPN & app user certificate*, then choose *OK*.

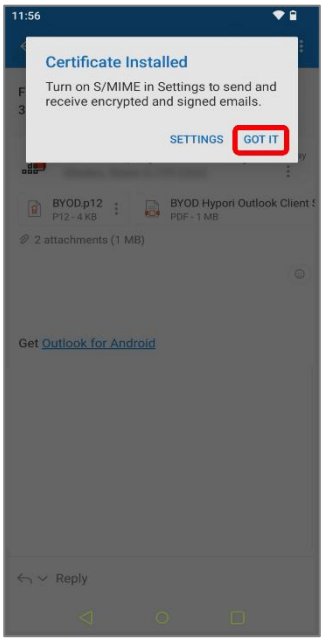


6. When prompted to *Name this certificate*, use the default certificate name. Select *OK*.



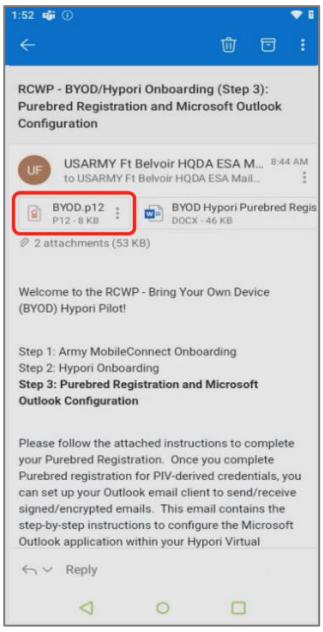


7. When prompted to *Choose certificate*, select the *Purebred Digital Signature Certificate*, then choose *Select*.

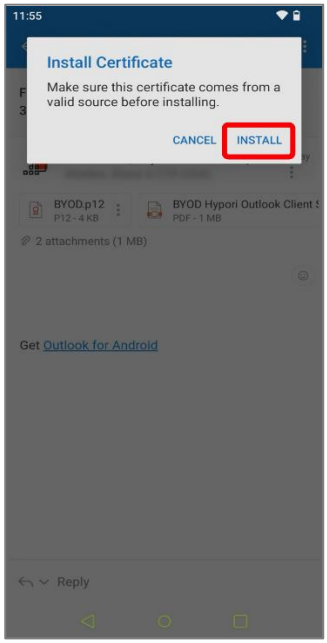


8. You will be notified that the *Certificate Installed*. While the message will instruct you to turn on S/MIME in Settings, you will complete this step later. Select *Got It*.

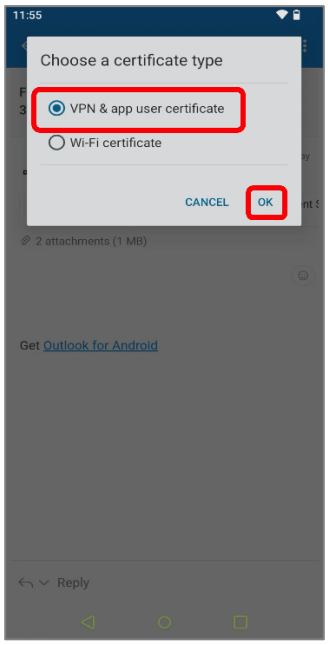
9. Next, install any recovered PKCS #12 certificates. Select the Hypori email's .p12 attachment to begin.



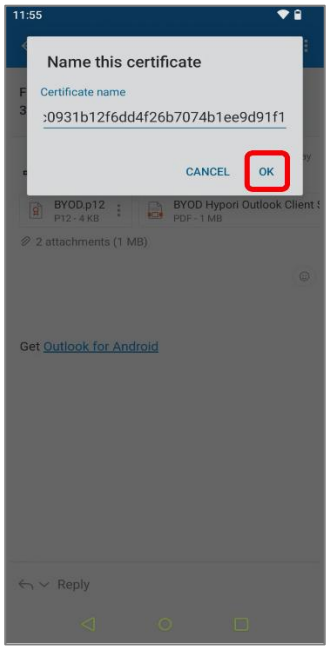
10. Select *Install*.

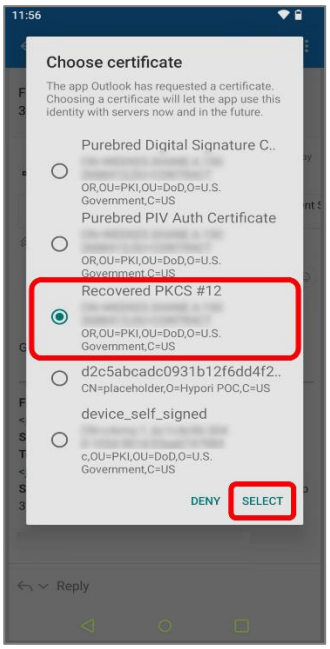


11. When prompted to *Choose a certificate type*, select *VPN & app user certificate*, then choose *OK*.



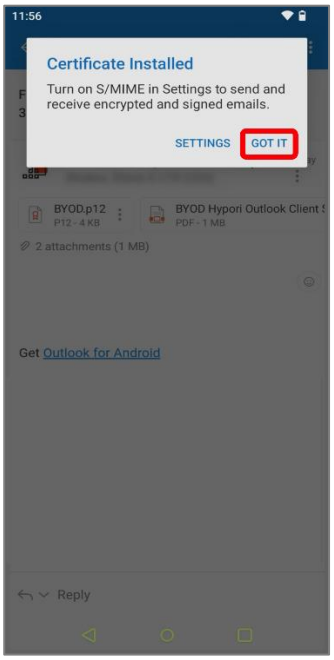
12. When prompted to *Name this certificate*, use the default Certificate name. Select *OK*.





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

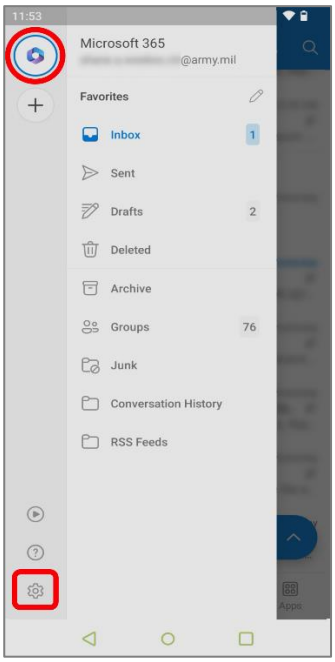
Note: If there is more than one Recovered PKCS #12 certificate here, take note because you'll have to complete this process for each one.



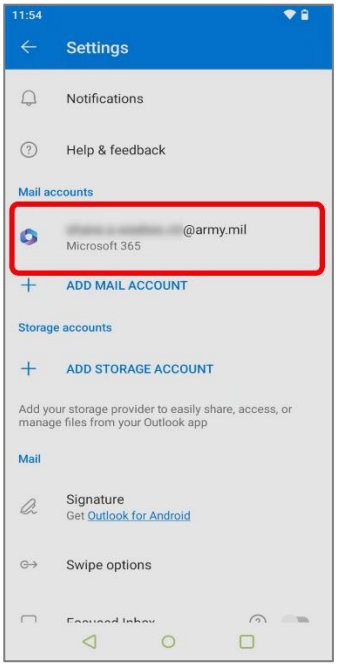
14. The *Certificate Installed* successfully.

a. If there are additional Recovered PKCS #12 certificates that must be added, select *Got It* and return to step 9.
b. If there are no additional Recovered PKCS #12 certificates that must be added, select *Settings* and continue to step 16.
c. After completion of certificate installation press the back arrow to close the email.

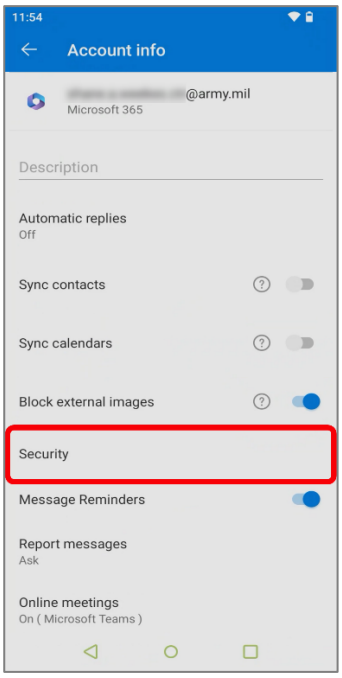
15. To confirm the download of the new certificates, click on The Settings menu by selecting the Office365 logo, then selecting the settings gear.



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



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



18. In the *Certificates Installed* section, you will see the new entries for the digital signature and for each recovered PKCS #12 certificate.