# D2A 6.0 Certificate replacement process

24 September 2025

# D2A 6.0 Certificate replacement process

## Certificate transition context

The **current D2A client certificate** will remain active until **8th October 2025,** the certificate will be deactivated at approximately 7:00am.

Once the current certificate is deactivated, the **new D2A Server certificate** will be installed on the **D2A server**, which will be configured to accept the **new D2A client certificate.**

If you have any return submissions scheduled **on or before 8th October**, please continue using the **current D2A client certificate**.

***Do not replace it until your data has been submitted.***

**Please note:** The switch from the current client certificate to the new client certificate will be a **hard cutover,** once the new client certificate is installed, the **current one will stop working immediately**.

Please follow the below steps to install the **new client certificate**

1. Close the D2A client application (if it is running)

2. Go to the D2A folder, the default location is C:\D2A
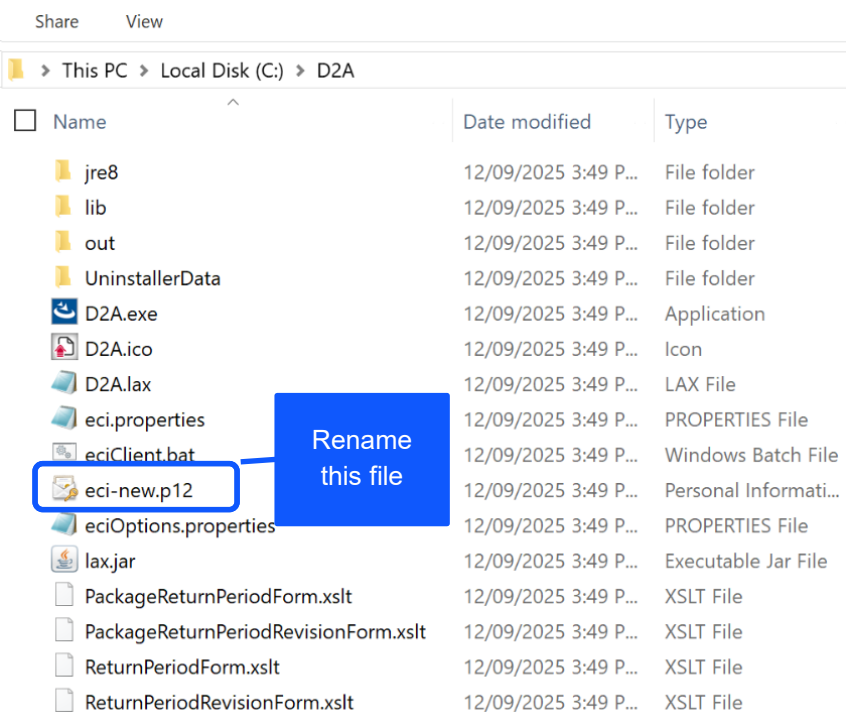


3. Rename the current certificate file from "eci-new.p12" to "eci-new-1.p12"

4. Download the new certificate from the APRA website

---

5. Right click the downloaded zip folder and select **Unzip or Extract** from the menu. You should see the below file after the folder has been unzipped
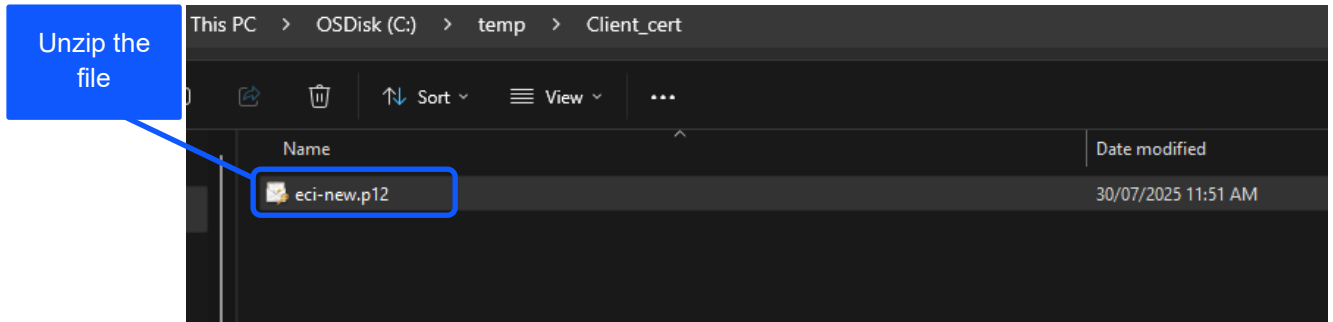


6. Copy and paste the "eci-new.p12" file from your unzipped folder to the D2A folder
7. Open the **eci.properties** file in the D2A folder to edit the password value
8. Search for the line called "cipher.keystore.initial.password" and then update the value from "changeMe" to "Apra@202507*352" and save the file

**Note:** you can press the CTRL+F keys on your keyboard to prompt the search field to appear

9. After all the changes, your eci.properties file and installation directory should look like below
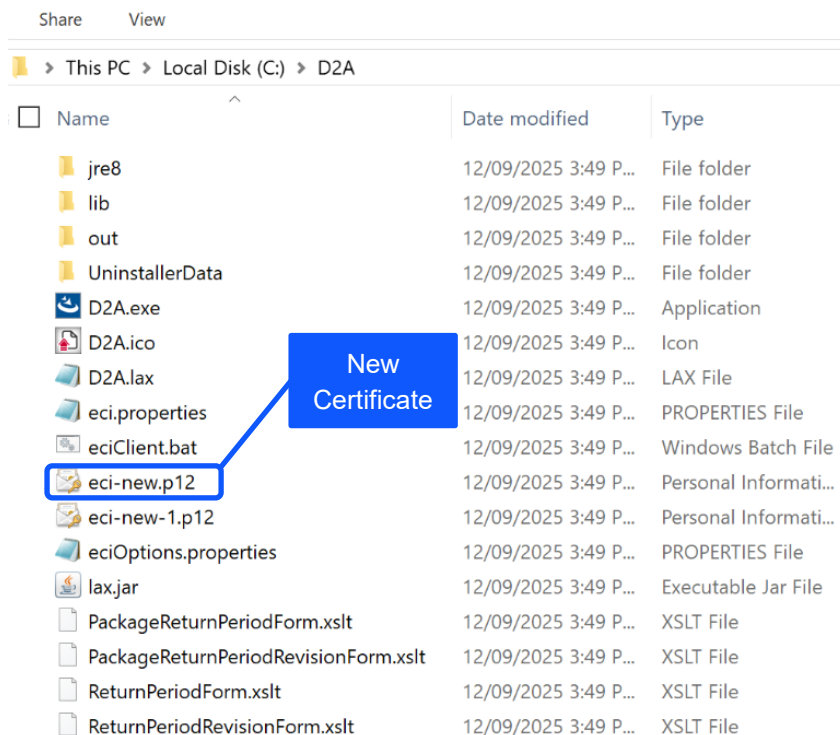
10. To confirm the certificate upgrade has been successful, open the D2A application, click the Tools menu at the top of the window, select "Request All New Blank Forms" and follow the prompts to refresh your forms. If your forms refresh successfully then the certificate has been successfully updated