LLOYD'S

CMR Offline Validation Tool
04 November 2024

Installation instructions

Installation Instructions

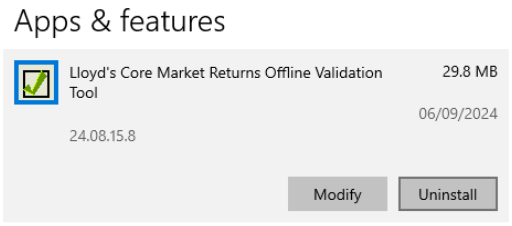
Whenever a new version of the Offline Validation Tool is published, it must be manually installed using the following installation instructions.

NOTE: A CMR user account is required to download the Offline Validation tool from the CMR website

1. If you have previously installed the Offline Validation Tool, it should be removed before continuing.

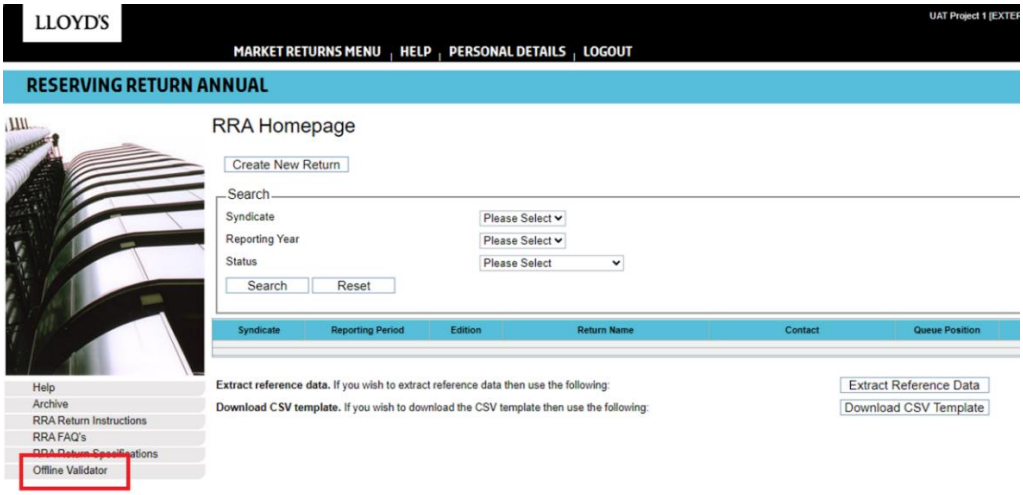
   Go to “Settings” and then “Apps & features”. Select “Lloyds Core Market Returns Offline Validation” and click **“Uninstall”**.

   The exact appearance and location of the uninstallation option will depend on your version of Windows. An example is shown below:

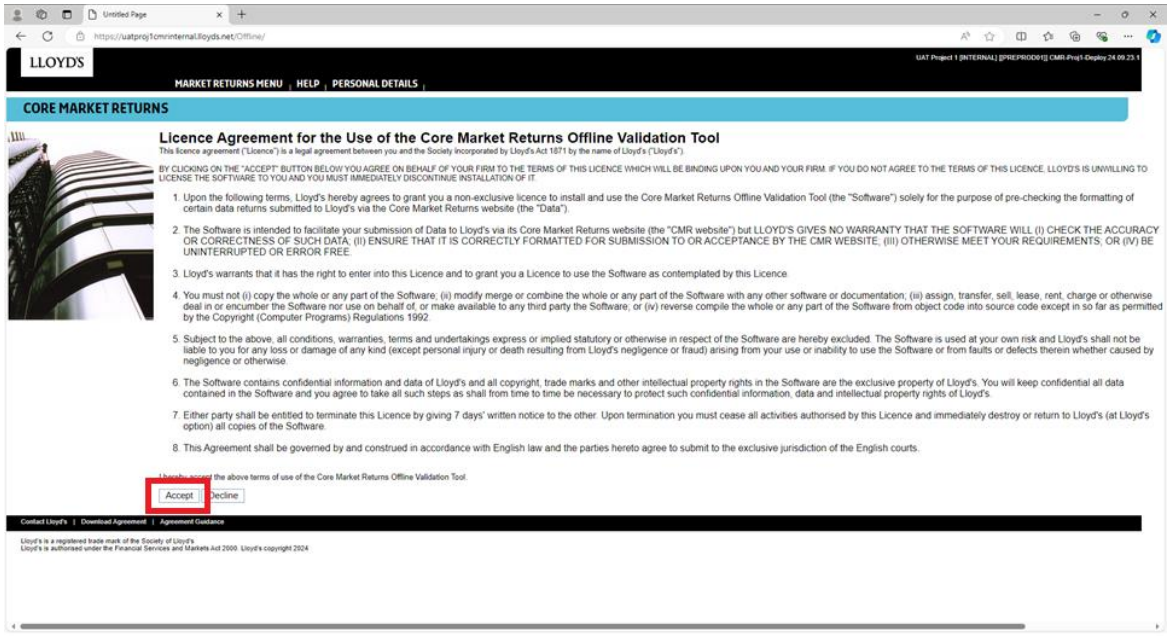


2. Once you have deleted any previous versions, download and install the file **CoreReturnsOffline.msi** via **https://cmr.lloyds.com/Offline**

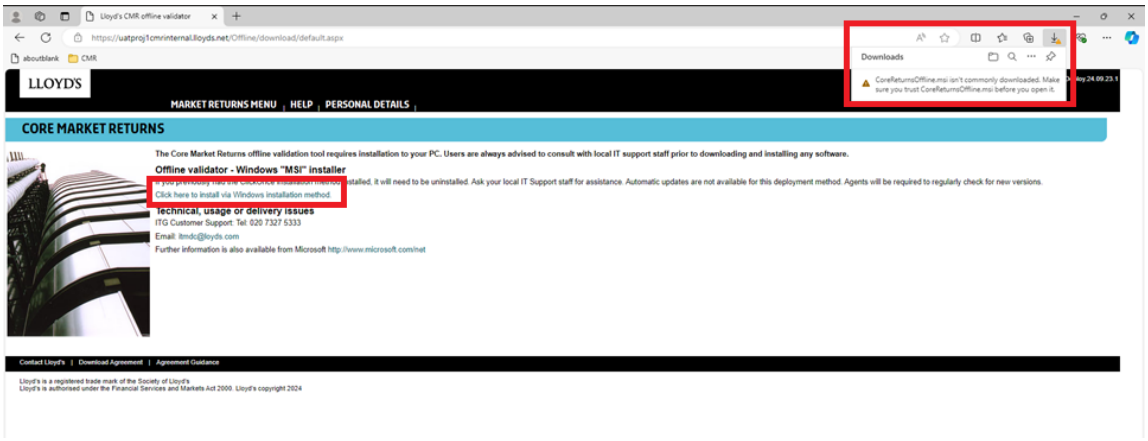
3. You can also download the file by logging into the CMR site **https://cmr.lloyds.com** and selecting **“Offline Validator”** in RRQ/RRA home page menu on the bottom left:



4. To download, first click to **“Accept”** the Licence Agreement:



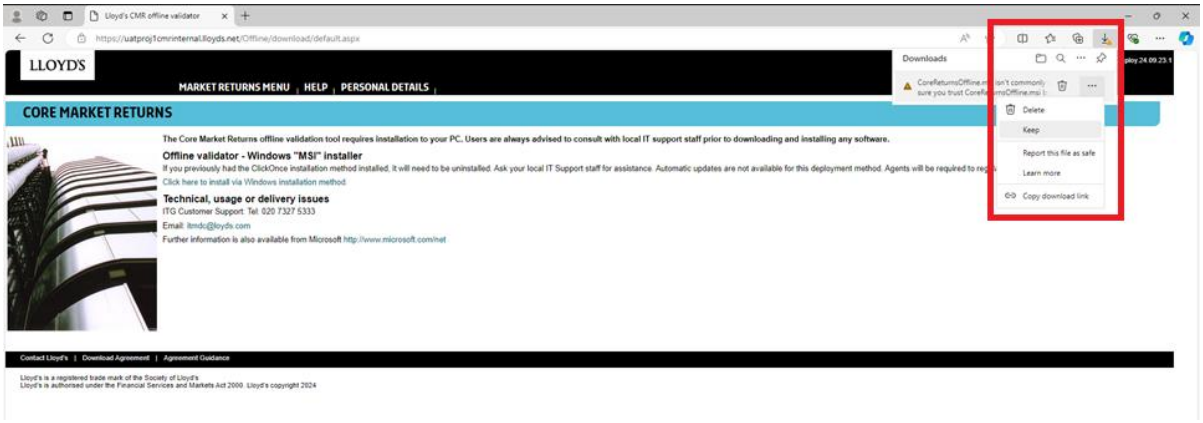
5. Then select **"Click here to install via Windows Installation method"** on the main menu.



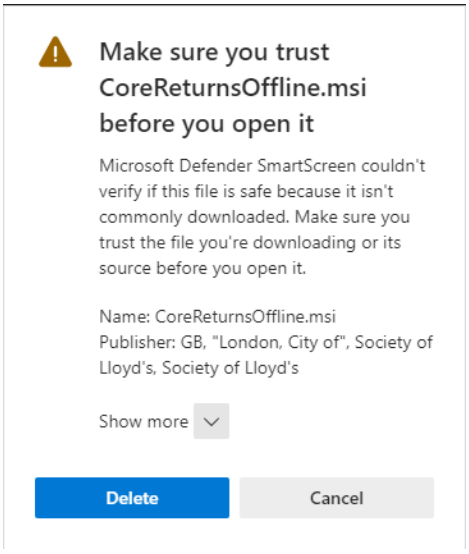
In the top right-hand corner of the screen, the Windows Defender Smart Screen will display a confirmation message:

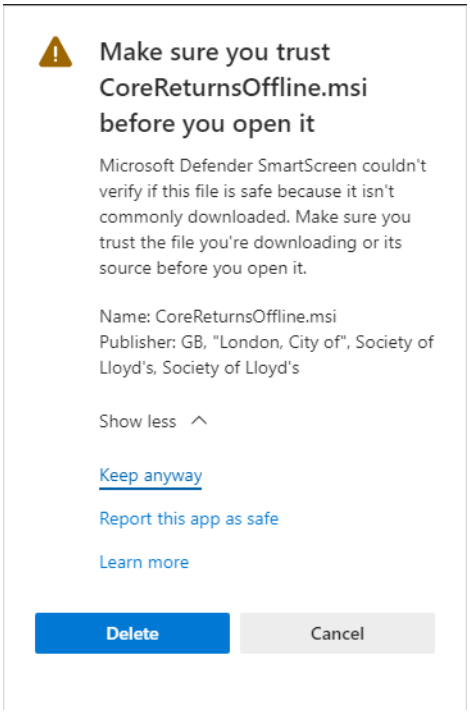
"CoreReturnsOffline.msi isn't commonly downloaded. Make sure you trust CoreReturnsOffline.msi before you open it"

6. Right click on the 3-dot menu on the right hand side of the screen and select **“Keep”**

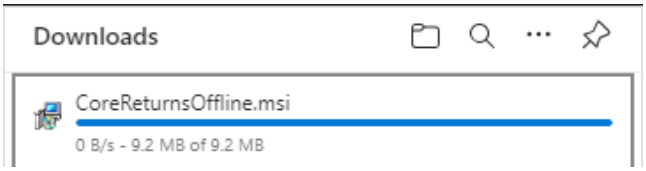


7. You will then see a further Windows Defender Smart Screen message. Click the down arrow next to **“Show More”** then choose **“Keep anyway”**

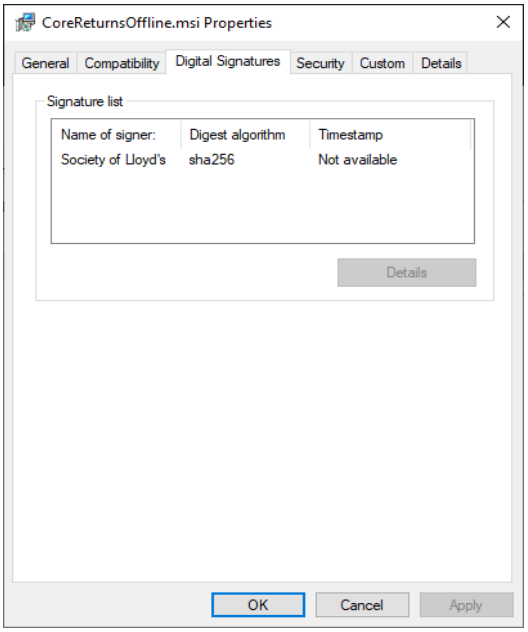




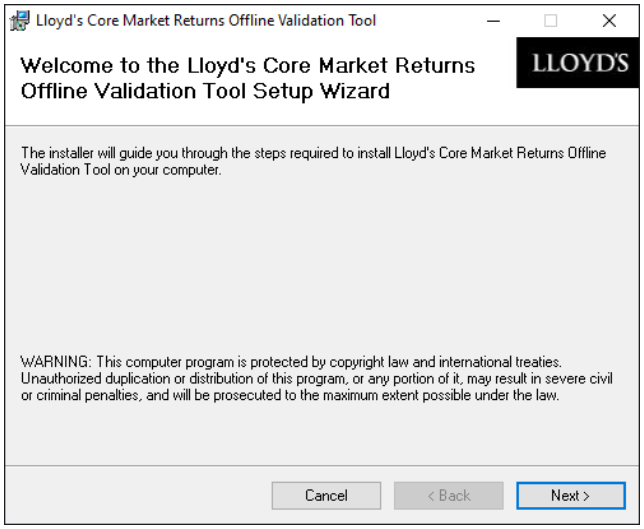
The download will now begin:



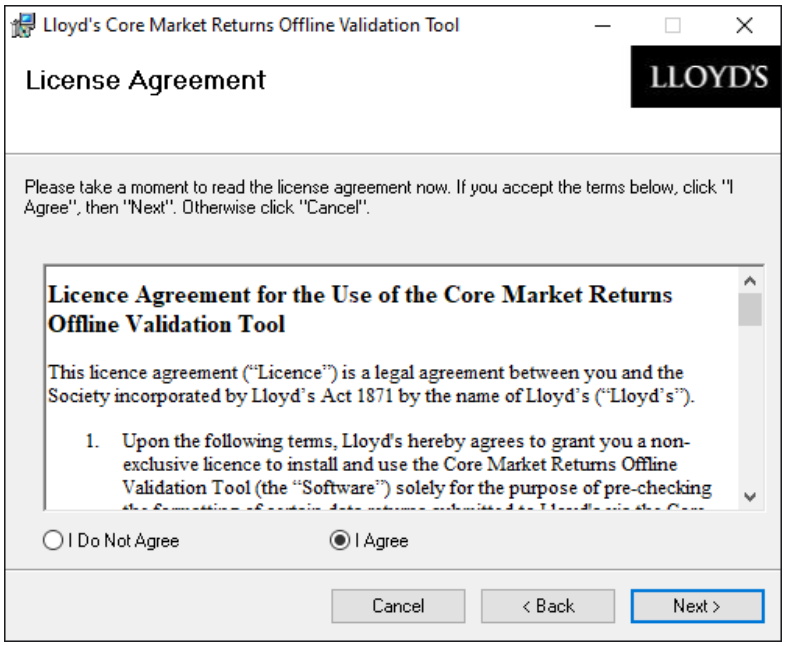
8. Once the download is complete, please confirm the Society of Lloyd's digital signature within the file properties.



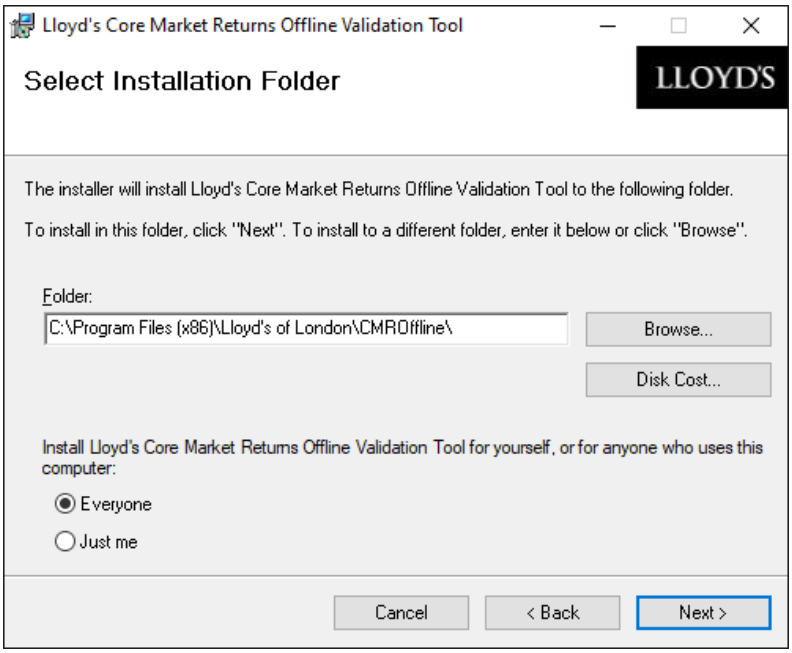
9. Open the file to begin the installation process, then click "Next" to continue.
NOTE: Administrator access is required to install the Offline Validation Tool. You may need to contact your IT Support team.



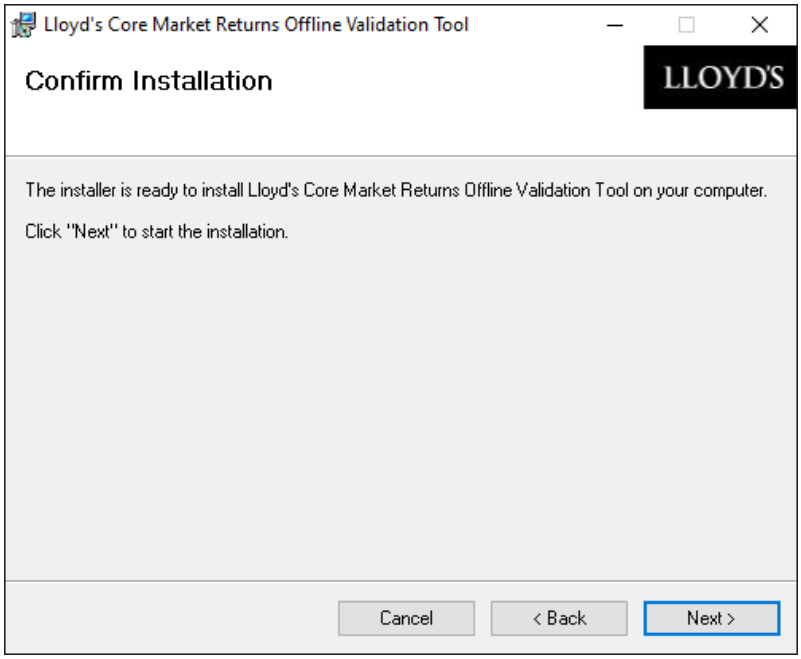
10. Review and accept the Licence Agreement by clicking **“I Agree”** and then click “Next” to continue.



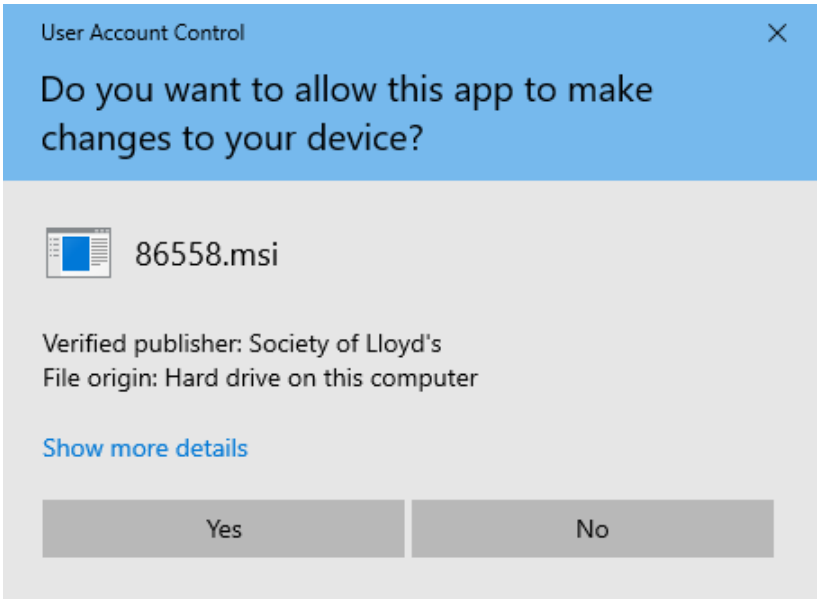
11. A default installation folder is displayed. Choose another folder if required or click “Next” to continue.



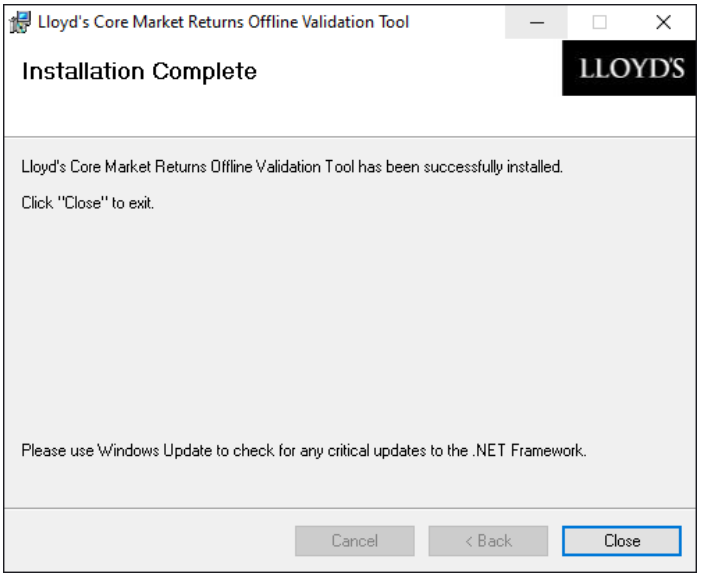
12. Confirm the installation by clicking “Next”



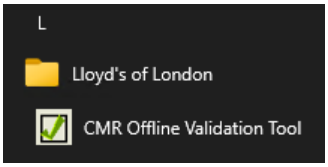
A security prompt will be displayed. Click “Yes” to continue:

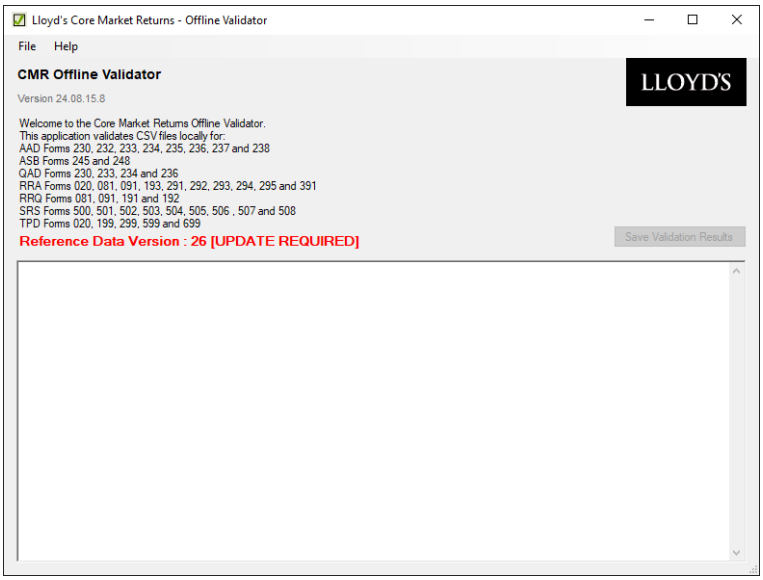


13. Once the installation is complete, click **“Close”** to end the installation process. If a new version of the Offline Validation Tool is published, it must also be manually installed by following these instructions.



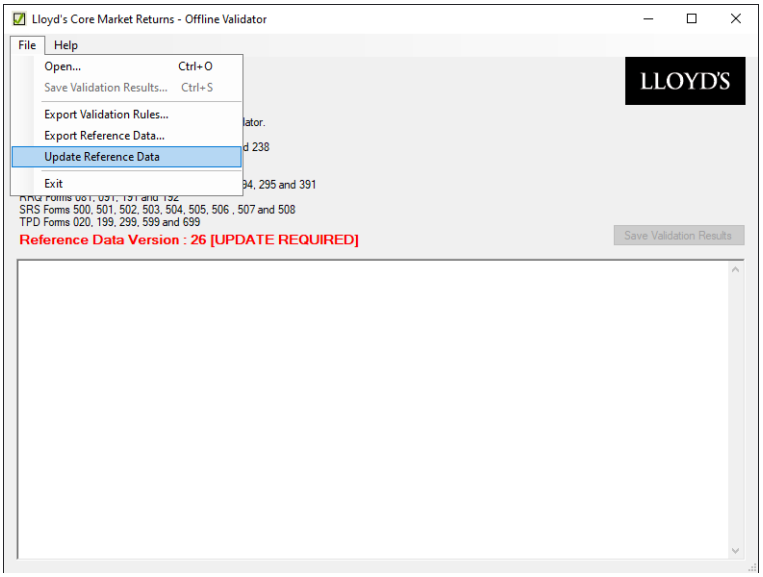
14. The **“CMR Offline Validation Tool”** can be found on and launched from the ‘Start’ menu:





15. Reference Data **must be updated** the first time that the Offline Validation Tool is launched.

NOTE: This update may take several minutes. Please <u>do not close the window</u> until you see confirmation that the update has been successful.



LLOYD'S

Microsoft Defender SmartScreen
Frequently Asked Questions (FAQs)

1. **What does it mean when Microsoft Defender SmartScreen marks a downloaded program as 'not commonly downloaded'?**
   Microsoft Defender SmartScreen uses information from Internet Explorer, Microsoft Edge, and Windows users around the world as well as anti-virus results, download volumes, download history, URL reputation, and many other criteria to determine the likely risk of downloaded programs. For example, programs that are downloaded by many users over a long period of time without a history of malware are not likely to be malicious.

   This warning indicates that caution should be taken before running the downloaded program, especially if the download is not digitally signed.

2. **Does this warning mean the file is malicious and will harm my computer?**
   No. The Application Reputation warning is not an indication that the download is malicious. However, for the average Internet Explorer, Microsoft Edge, and Windows user this warning is usually associated with a download that may have a higher risk of being malicious.

3. **How should I decide whether to run a program flagged by Microsoft Defender SmartScreen as 'not commonly downloaded'?**
   There are several factors to take into consideration before running a program flagged by Microsoft Defender SmartScreen:

   - Is the file digitally signed by a software publisher? The application reputation warning dialog will indicate if the file is not digitally signed. Most malicious programs are not signed by a publisher so be careful if you choose to ignore the warning.

   - How were you directed to this download? Was the download link unsolicited, such as from an email, instant message, or social networking post? If the download link was unsolicited - even if it looks like it's from someone you trust - it is more likely to be malicious.

   - Would you expect this program to be an uncommon download? If you thought you were downloading a popular game or other program, you should be suspicious that many other Internet Explorer users have not also downloaded the program.