DLA Information Operations
"How To" Guide

OPR: J63B

Date Updated: 06/12/25

Keywords: VDI, Citrix, Certificates

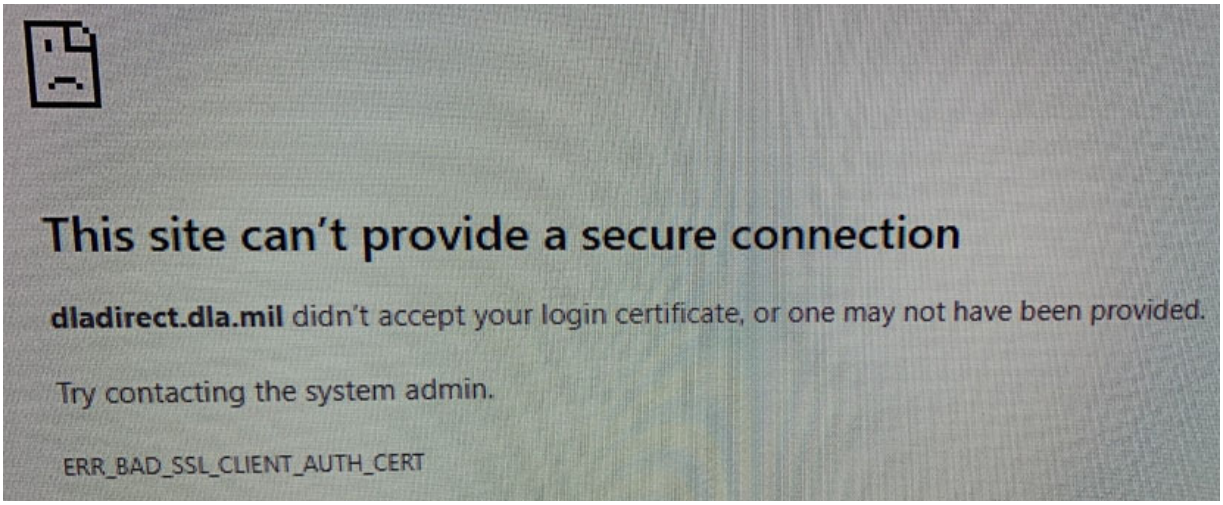
Op Cat: Update/ Knowlege / External use

Prod Cat: Software / Infrastructure Services / Virtualization

---

How to Install InstallRoot 5.6

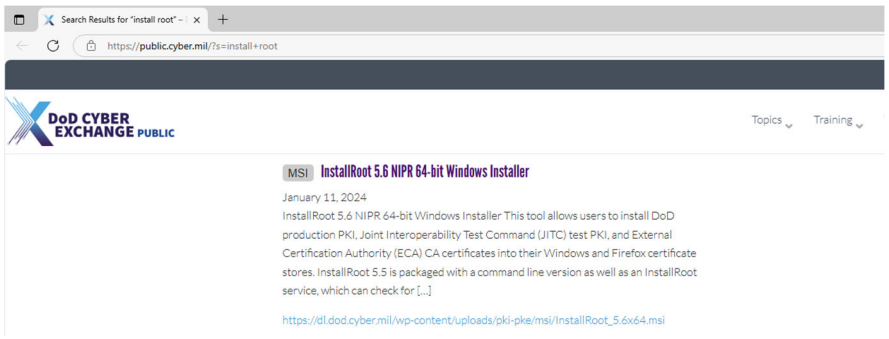
Some users may intermittently experience connection errors when authenticating to Citrix Storefront. An example error most commonly seen is shown below:



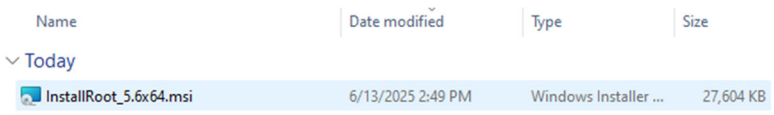
If you receive this error, please follow the steps below to install InstallRoot 5.6. This will install the latest DoD Root Certificates on your local machine.

Installing InstallRoot 5.6

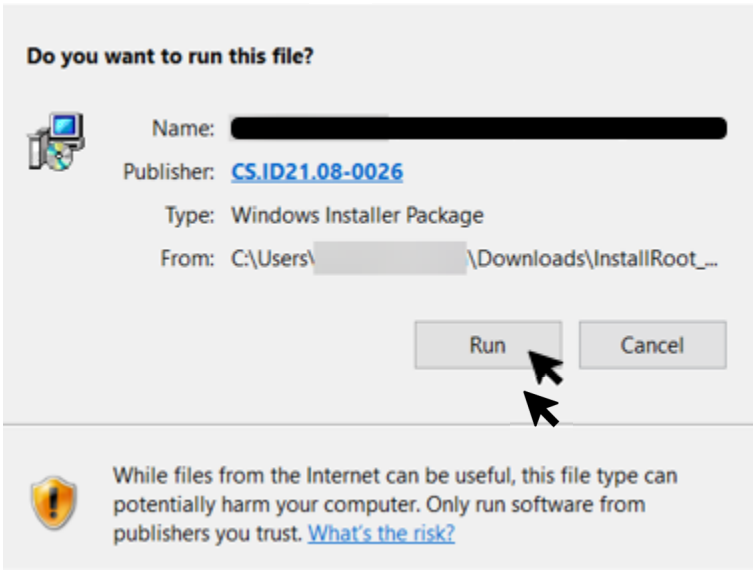
1. Download the latest version of InstallRoot (5.6) from https://public.cyber.mil/?s=install+root



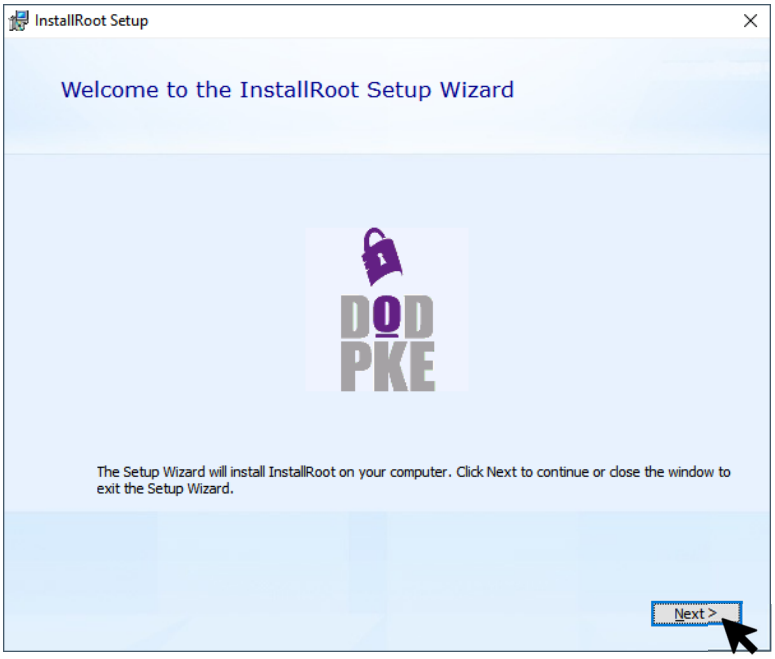
2. Navigate to the Downloads folder on the local machine, and double click the installer file.



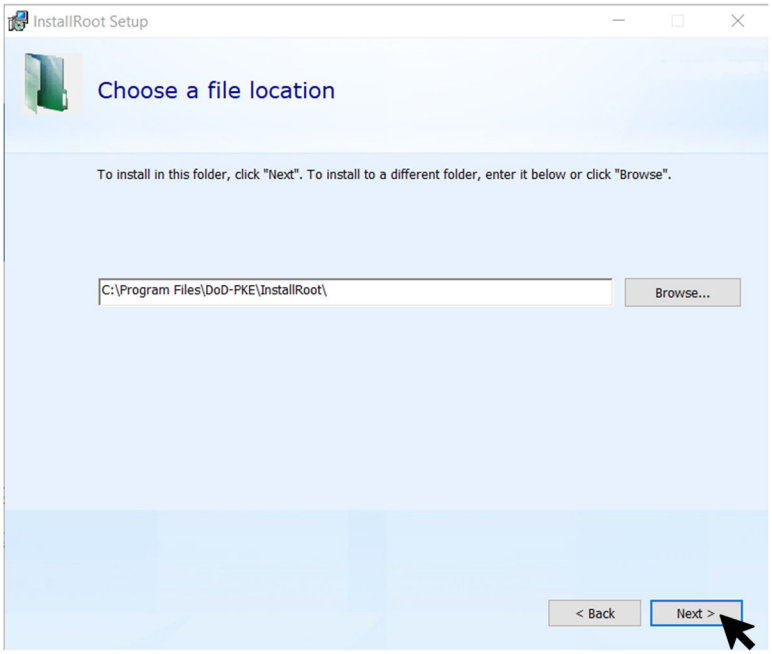
3. Click **Run** at the next screen.



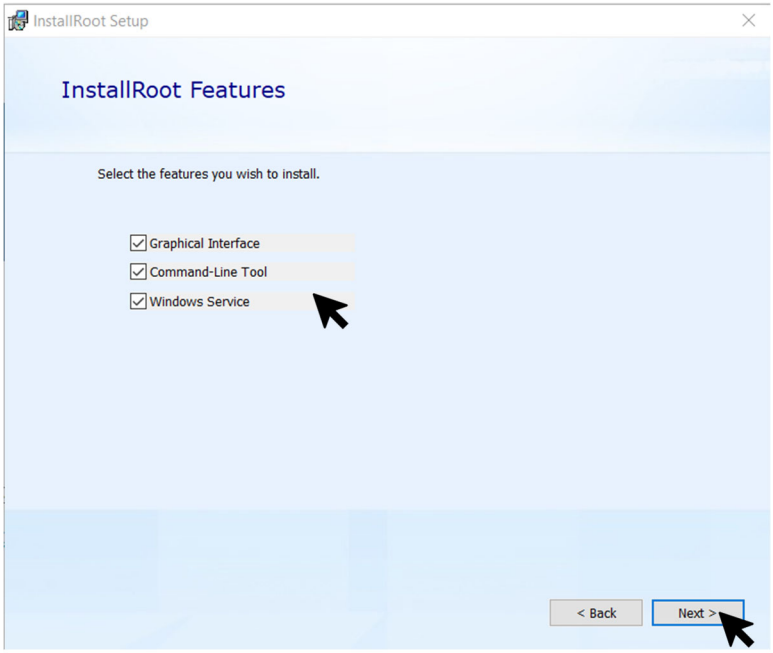
4. On the InstallRoot Setup screen, click **Next** >.



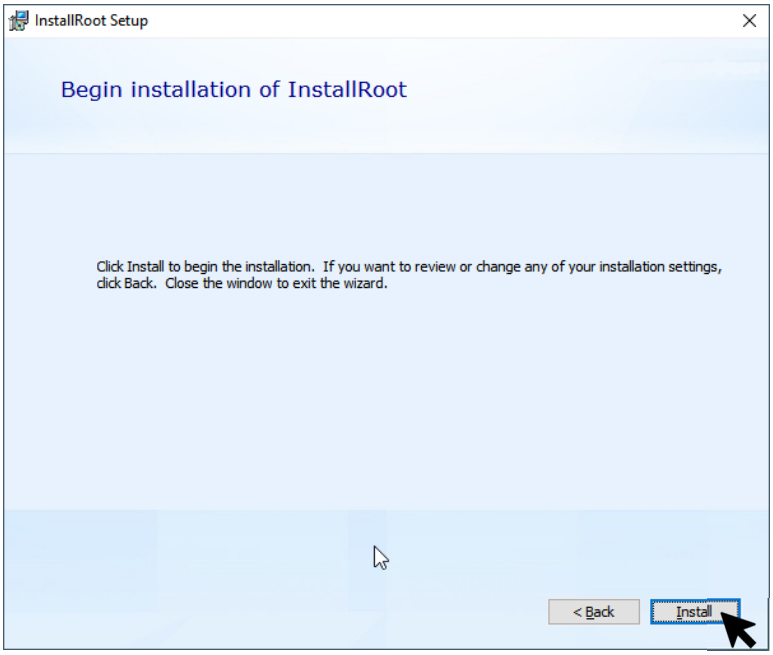
5. Select the desired installation location. It is recommend to use the default folder location. Click **Next** >.



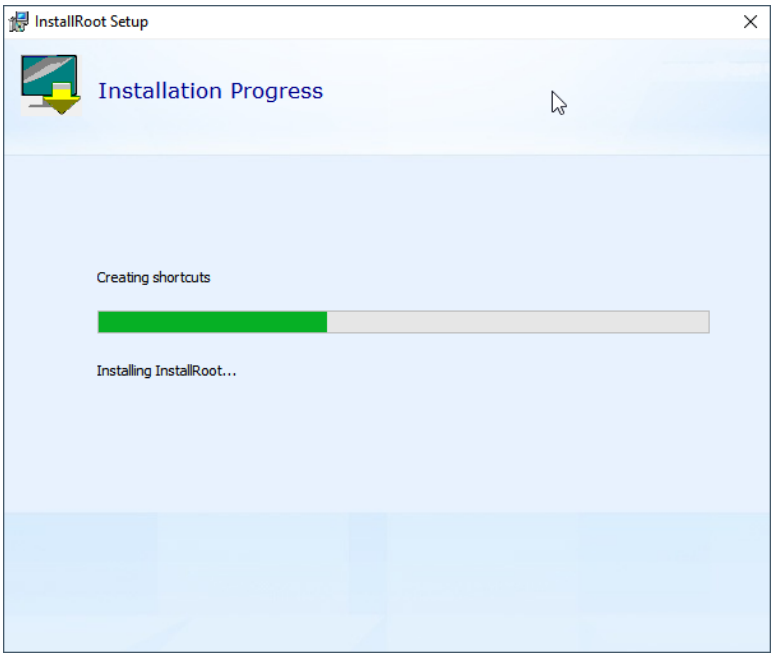
6. Under InstallRoot Features, leave all default options selected. Click **Next >**.



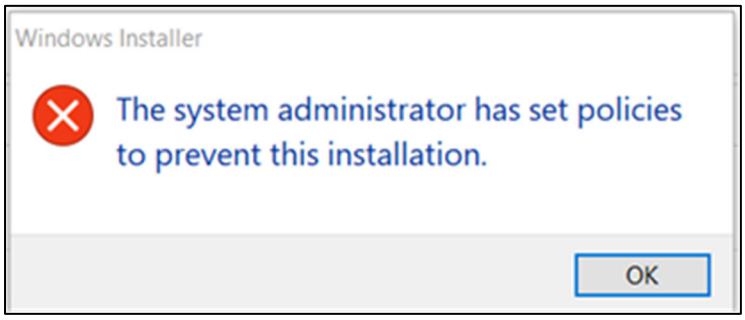
7. On Begin installation of InstallRoot screen, click **Install**.



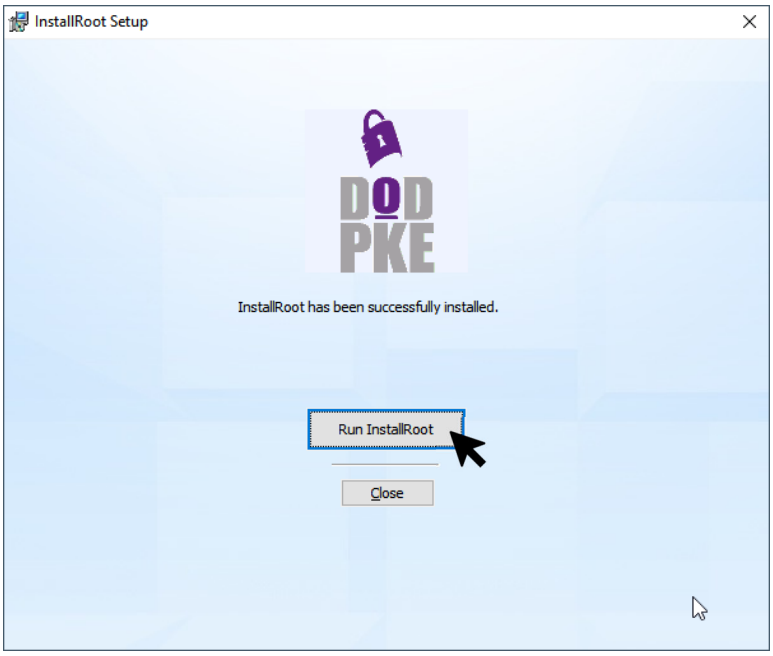
8. The Installation Progress screen will appear. The installation may take several minutes to complete. You may be prompted by a User Account Control pop up, select **Yes**.



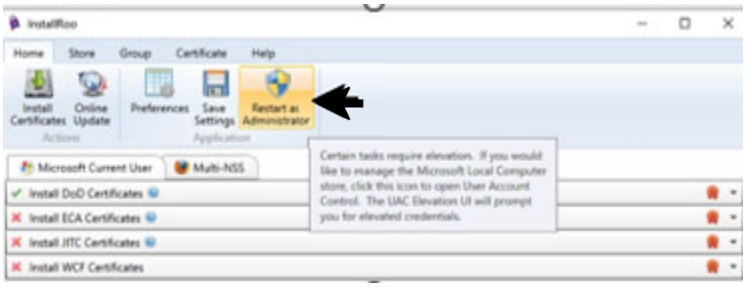
9. Some users may experience the installation errors stating they do not have permissions to proceed with installation. This most commonly happens on company-furnished equipment (CFE) endpoints. This should not happen as often on personally owned computers and endpoints. If users receive the message below, have the user contact their company IT Help Desk team to have them install this software with an Administrator account.



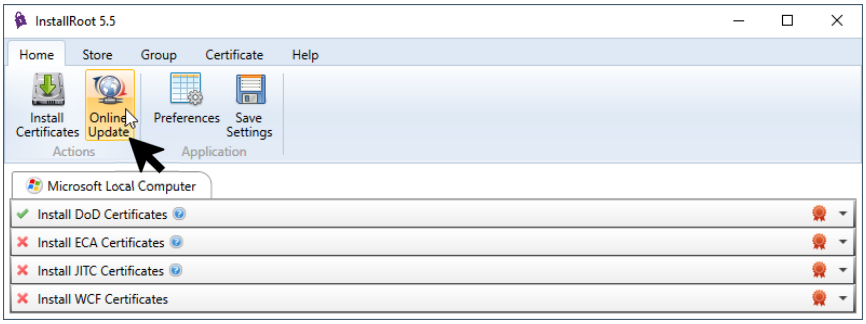
10. Once you see the “InstallRoot has been successfully installed message,” click **Run InstallRoot**.



11. Click **Restart as Administrator** to restart the application with Administrative privileges.

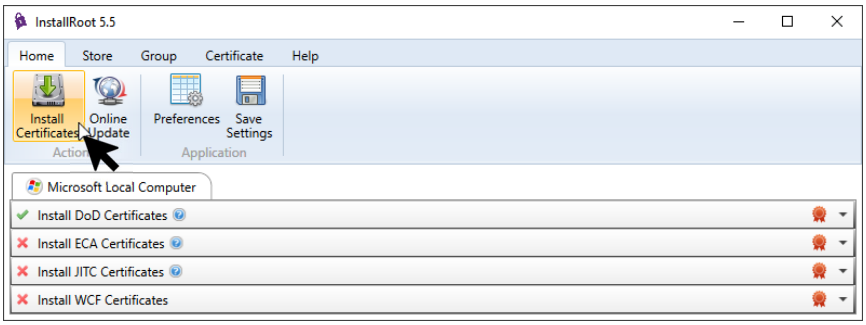


12. Click **Online Update** to check for any application and certificate updates. You should see a status message indicating whether any new updates were applied.

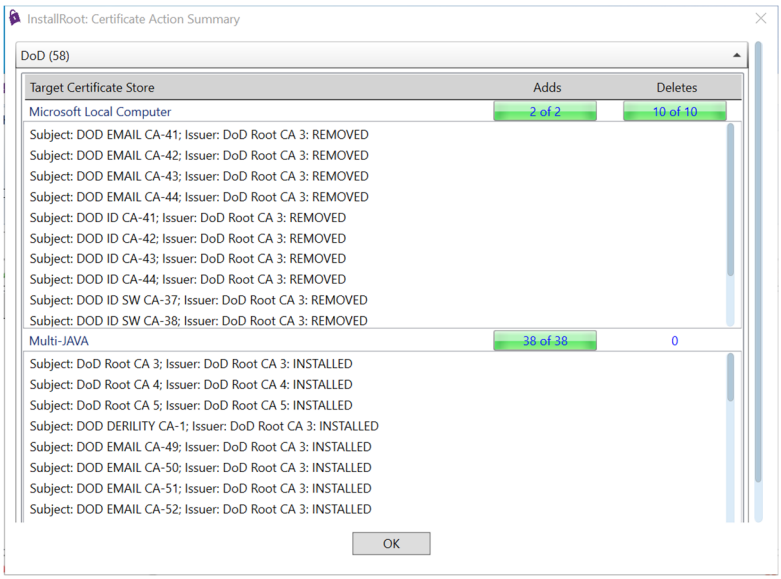


Once you click on Online Update, wait for any applicable certificate updates to download and apply. If no updates are found, you will see a message like the one below.

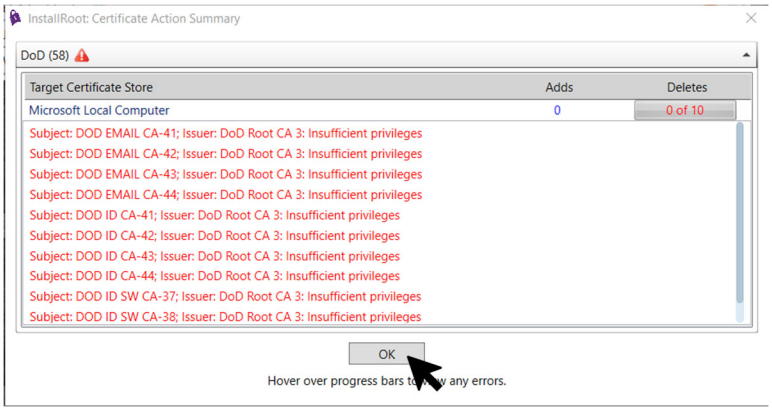
13. Click **Install Certificates**.



14. Once the certificates are installed successfully, you will see a “certificate installation successful” message. If the certificates were already installed, you may not see a message.



15. If you see the error below, click **OK** and attempt to have the user sign into Citrix Storefront. Seeing this error generally will not affect overall certificate installation, you may click OK to disregard. If they are still unsuccessful, please have the user contact their company IT Help Desk team to have them install this software with an Administrator account.



16. After installation is complete, close InstallRoot, reboot the endpoint and try to sign into VDI again. If the user still receives the aforementioned SSL error, have them contact their company's IT Help Desk team for further assistance (if on a CFE laptop). We do not officially support personally-owned home equipment. Alternatively, the user may also request a UMC laptop by submitting a request on the Service Portal.

Installing DigiCert Root Certificates

17. Additional root certificate installation may be required for home users connecting to External VDI. PKI is migrating us to a new root certificate vendor for our public certificates. You may need to download and install new root certificates to connect to External VDI from your at home device effective from the following dates.

OCONUS : Effective 06/09/2025

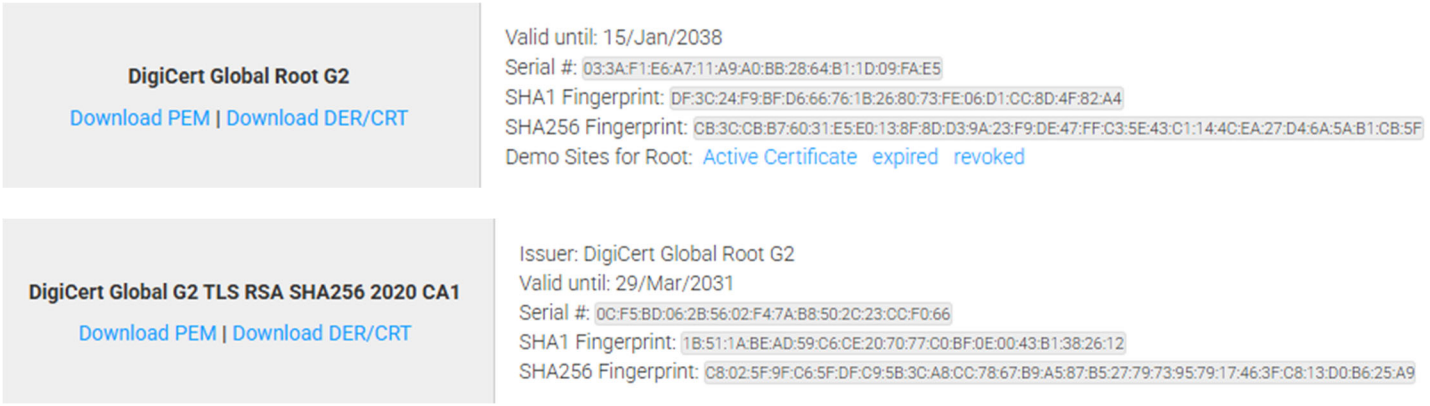
https://remote.pacific.dla.mil

https://remoteasia.pacific.dla.mil

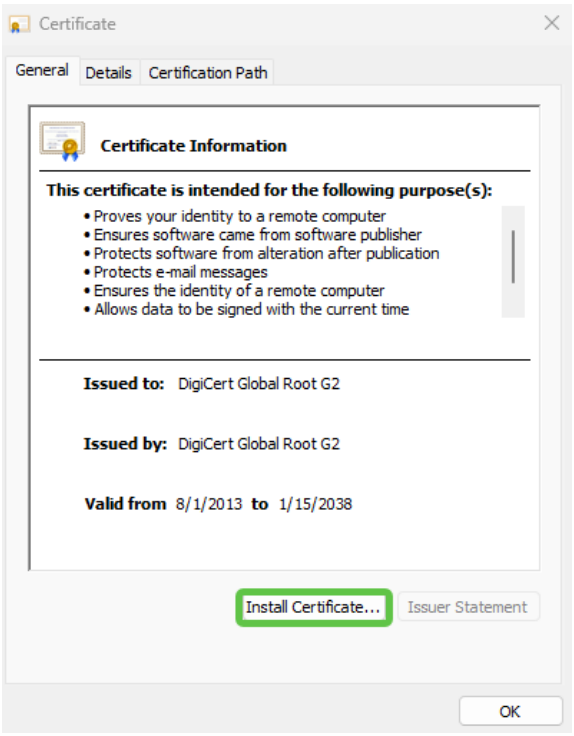
CONUS: Effective 10/06/2025

https://dladirect.dla.mil

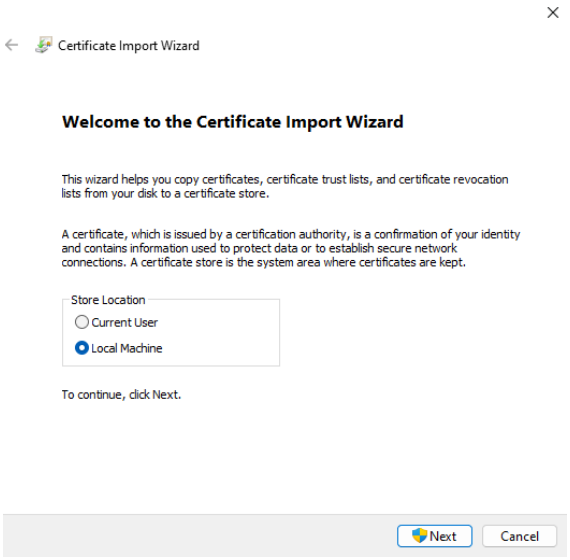
18. The following root certificate & intermediate root certificate **DigiCert Global Root G2** "Download DER/CRT" **DigiCert Global G2 TLS RSA SHA256 2020 CA1** "Download DER/CRT" needs to be downloaded on your endpoint. https://www.digicert.com/kb/digicert-root-certificates.htm



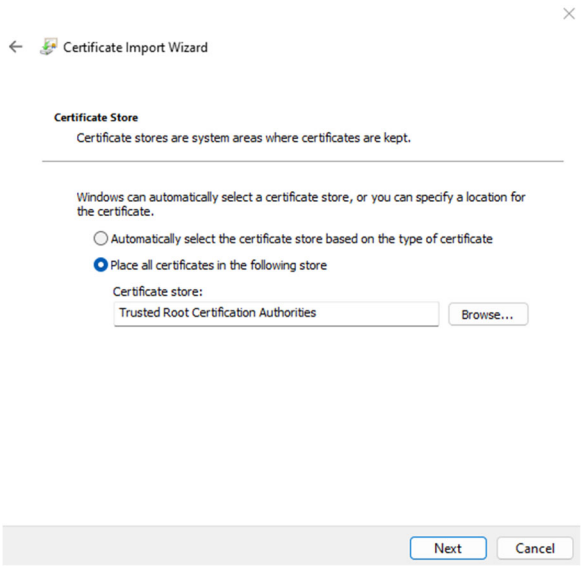
19. Double click the download certificate "DigiCertGlobalRootG2.cer" and choose "Install Certificate".



20. Choose “Local Machine”

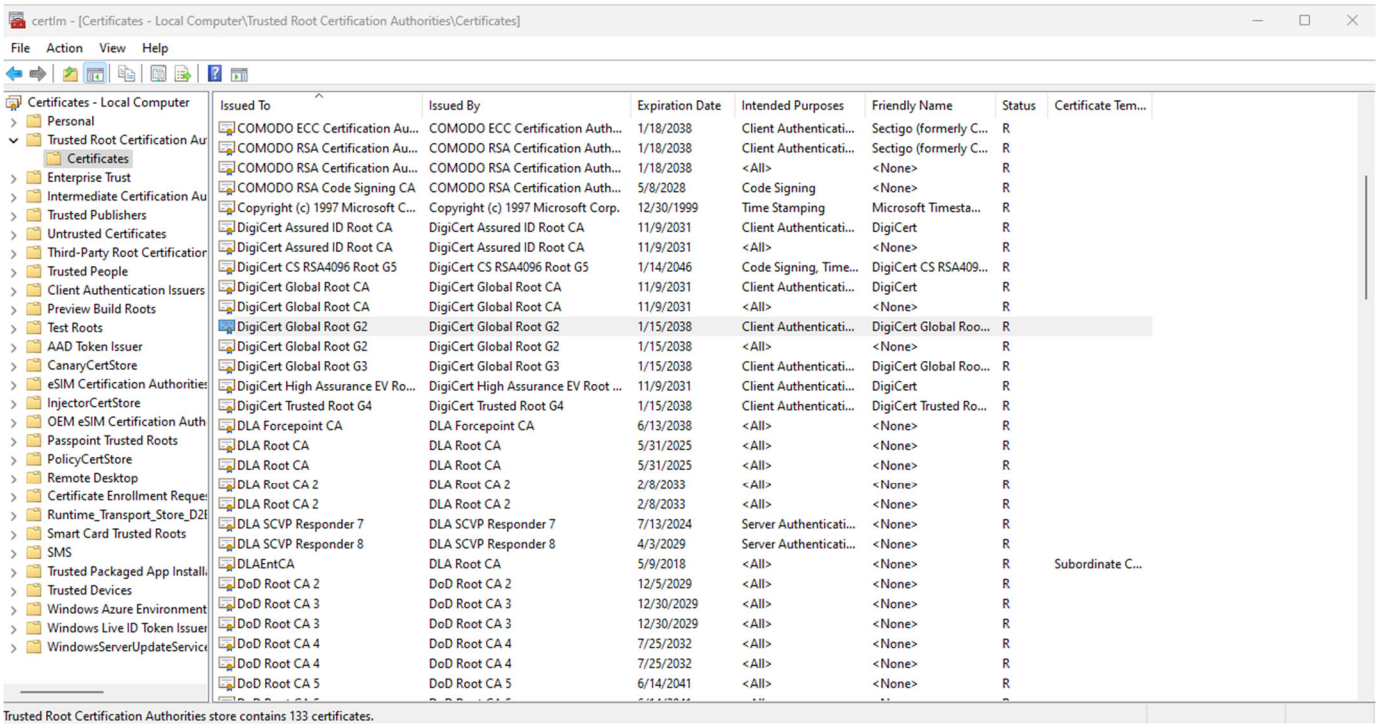


21. Choose “Place all certificates in the following store” and select “Trusted Root Certification Authorities”. Click Next then Finish.



22. You should now see the DigiCert Global Root G2 Root Certificate installed on your endpoint.

Directory: Trusted Root Certification Authorities | Certificate Name: DigiCert Global Root G2



23. Repeat installation steps for the intermediate certificate you downloaded **DigiCert Global G2 TLS RSA SHA256 2020 CA1** and place in the Intermediate Certification Authorities directory.

Directory: Intermediate Root Certification Authorities | Certificate Name: DigiCert Global G2 TLS RSA SHA256 2020 CA1