



DLA Information Operations “How To” Guide

OPR: J63B

Date Updated: 06/12/25

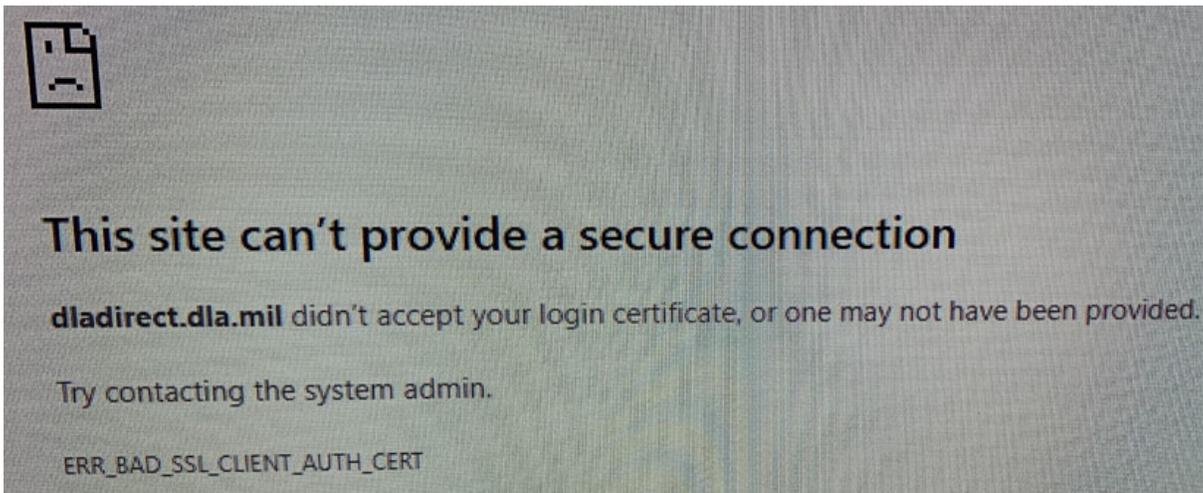
Keywords: VDI, Citrix, Certificates

Op Cat: Update/ Knowledge / 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

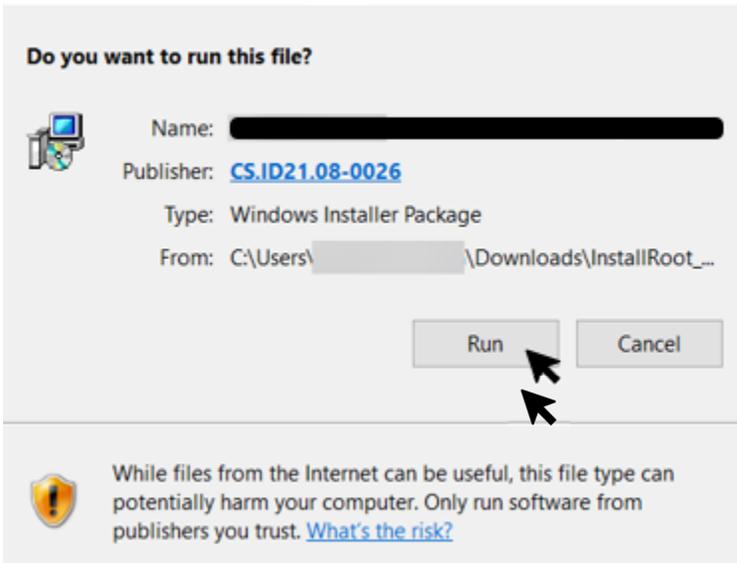
1. Download the latest version of InstallRoot (5.6) from <https://public.cyber.mil/?s=install+root>



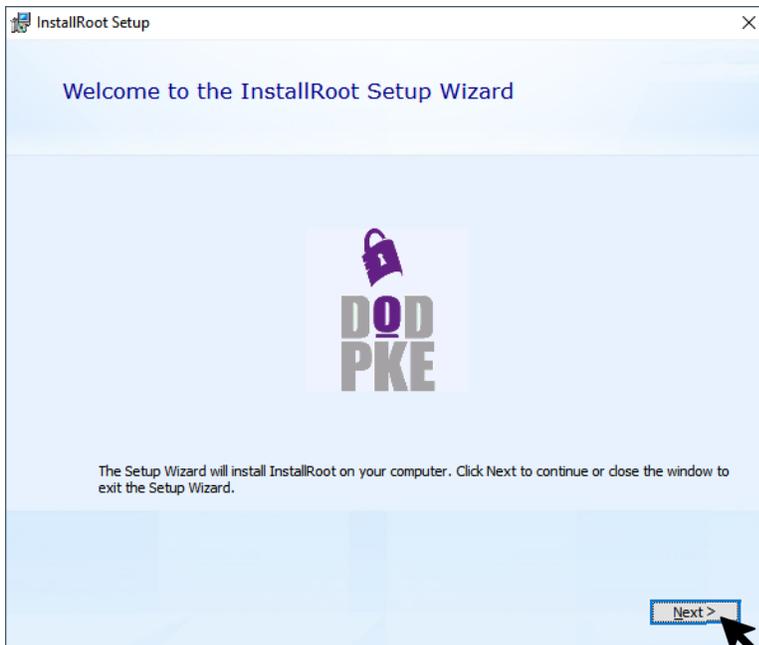
2. Navigate to the Downloads folder on the local machine, and double click the installer file.

Name	Date modified	Type	Size
▼ Today			
 InstallRoot_5.6x64.msi	6/13/2025 2:49 PM	Windows Installer ...	27,604 KB

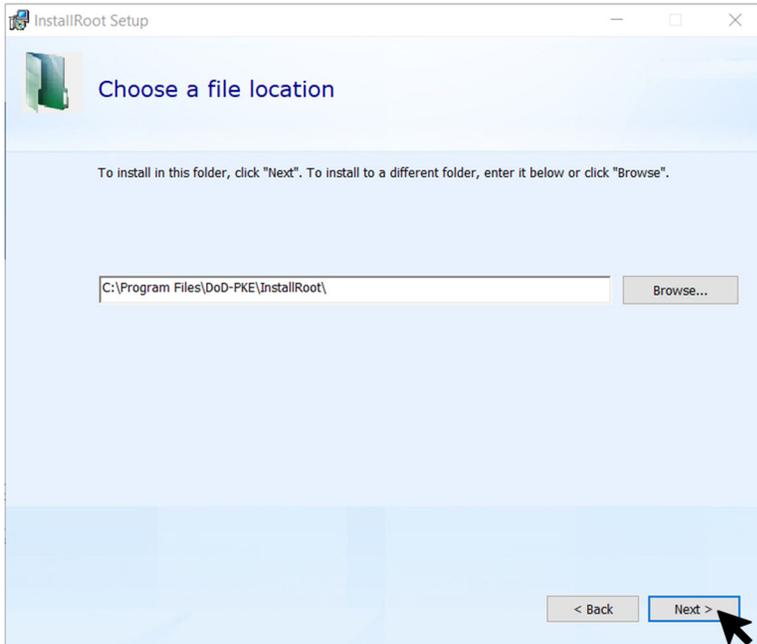
3. Click **Run** at the next screen



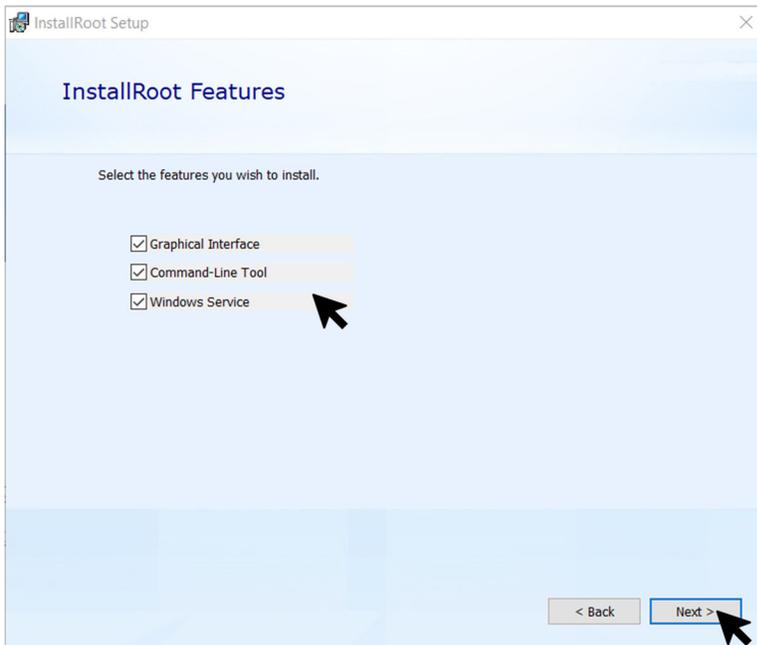
4. On the InstallRoot Setup screen, click **Next >**.



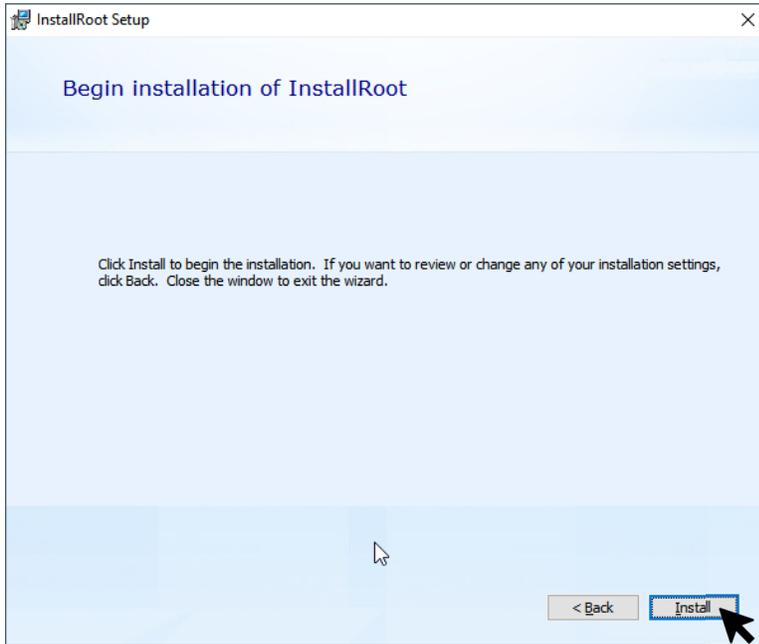
5. Select the desired installation location. It is recommend to use the default folder location. Click **Next >**.



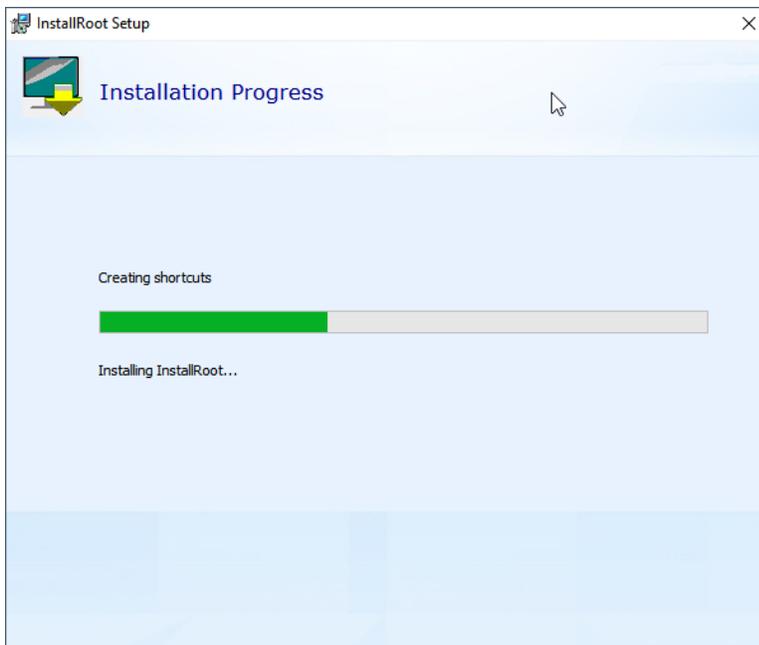
6. Under InstallRoot Features, leave all default options selected. Click **Next >**.



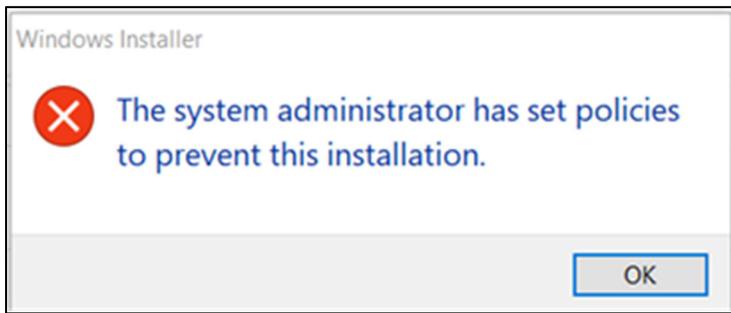
7. On Begin installation of InstallRoot screen, click **Install**.



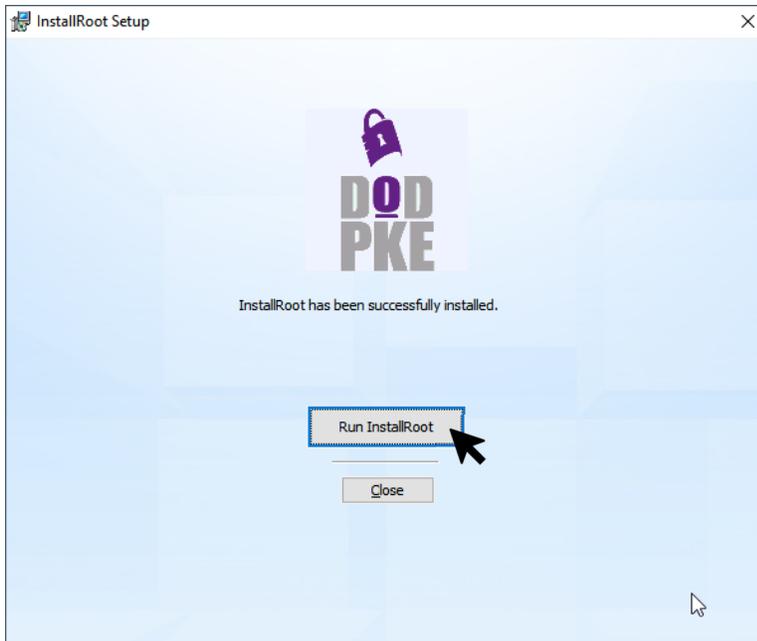
8. The Installation Progress screen will appear. The installation may take several minutes to complete. You may be prompted by a User Account Control pop up, select **Yes**.



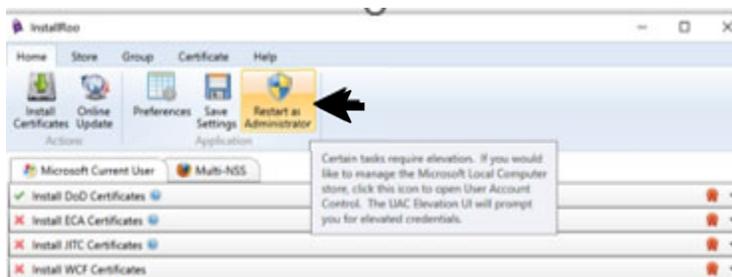
9. Some users may experience the installation errors stating they do not have permissions to proceed with installation. This most commonly happens on company-furnished equipment (CFE) endpoints. This should not happen as often on personally owned computers and endpoints. If users receive the message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



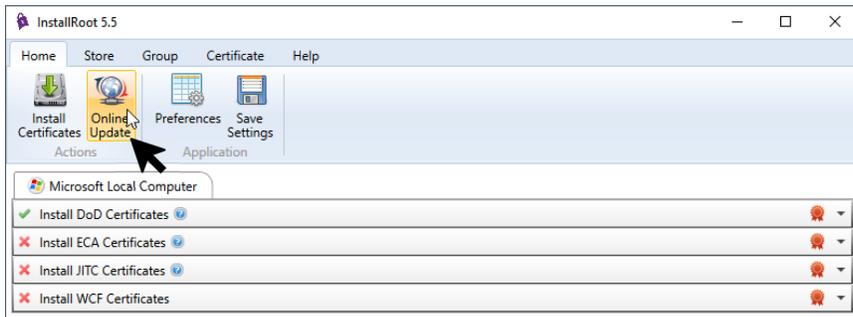
10. Once you see the “InstallRoot has been successfully installed message,” click **Run InstallRoot**.



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



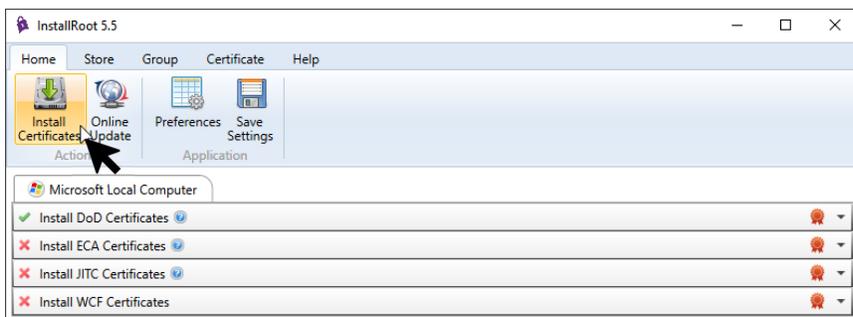
12. Click **Online Update** to check for any application and certificate updates. You should see a status message indicating whether any new updates were applied.



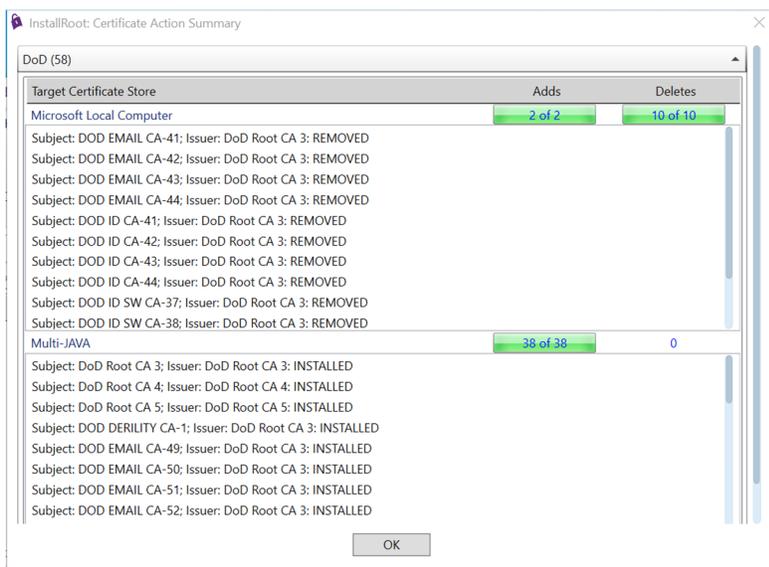
Once you click on Online Update, wait for any applicable certificate updates to download and apply. If no updates are found, you will see a message like the one below.



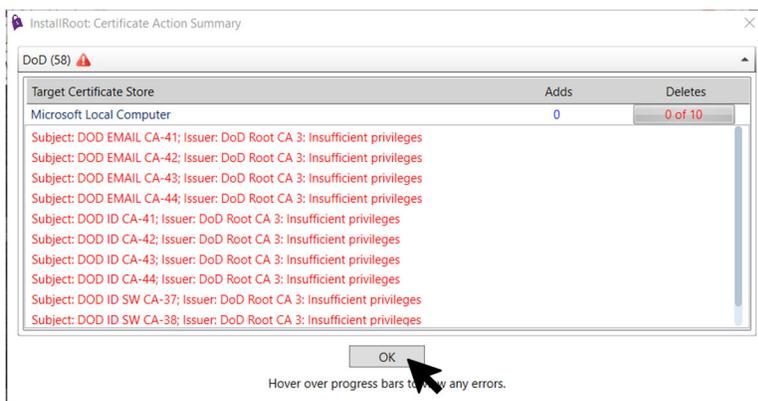
13. Click **Install Certificates**.



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://remotearia.pacific.dla.mil>

CONUS: Effective 10/06/2025

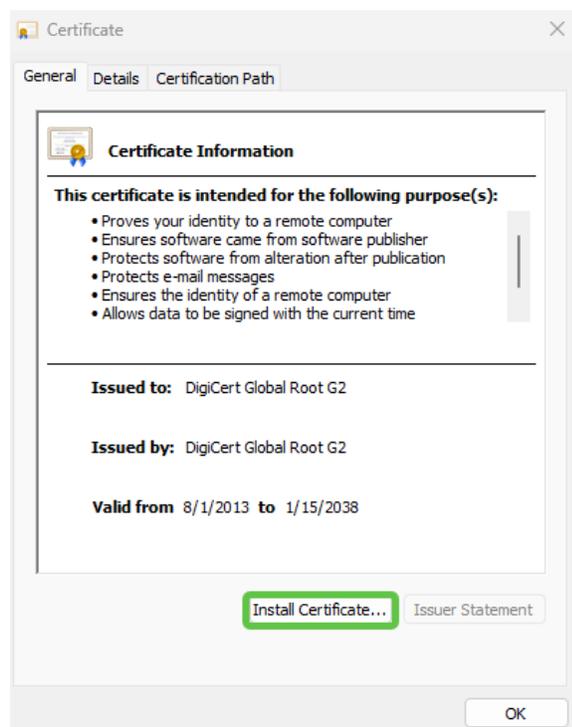
<https://dladirect.dla.mil>

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.

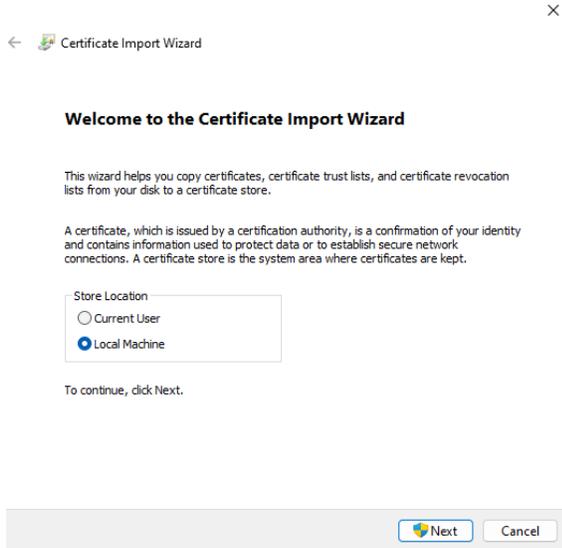
<https://www.digicert.com/kb/digicert-root-certificates.htm>

<p>DigiCert Global Root G2 Download PEM Download DER/CRT</p>	<p>Valid until: 15/Jan/2038 Serial #: 03:3A:F1:E6:A7:11:A9:A0:BB:28:64:B1:1D:09:FA:E5 SHA1 Fingerprint: DF:3C:24:F9:BF:D6:66:76:1B:26:80:73:FE:06:D1:CC:8D:4F:82:A4 SHA256 Fingerprint: CB:3C:0B:B7:60:31:E5:E0:13:8F:8D:D3:9A:23:F9:DE:47:FF:C3:5E:43:C1:14:4C:EA:27:D4:6A:5A:B1:0B:5F Demo Sites for Root: Active Certificate expired revoked</p>
<p>DigiCert Global G2 TLS RSA SHA256 2020 CA1 Download PEM Download DER/CRT</p>	<p>Issuer: DigiCert Global Root G2 Valid until: 29/Mar/2031 Serial #: 0C:F5:BD:06:2B:56:02:F4:7A:B8:50:2C:23:CC:F0:66 SHA1 Fingerprint: 1B:51:1A:BE:AD:59:C6:CE:20:70:77:C0:BF:0E:00:43:B1:38:26:12 SHA256 Fingerprint: C8:02:5F:9F:C6:5F:DF:C9:5B:3C:A8:CC:78:67:B9:A5:87:B5:27:79:73:95:79:17:46:3F:C8:13:D0:B6:25:A9</p>

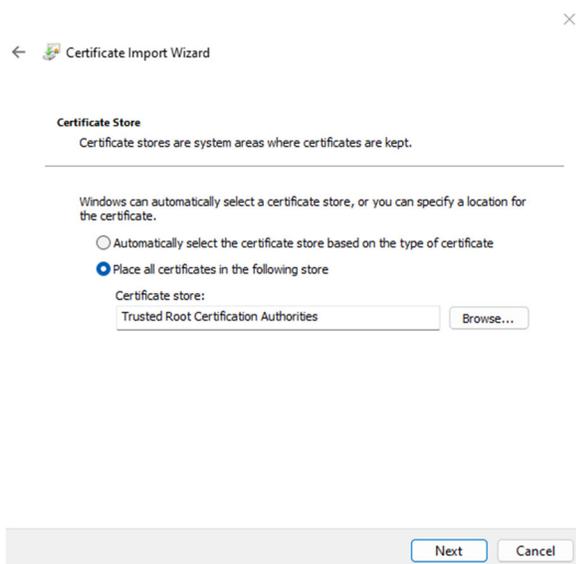
19. Double click the download certificate “DigiCertGlobalRootG2.cer” and choose “Install Certificate”.



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

certlm - [Certificates - Local Computer\Trusted Root Certification Authorities\Certificates]

File Action View Help

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
COMODO ECC Certification Au...	COMODO ECC Certification Auth...	1/18/2038	Client Authenticati...	Setigo (formerly C...	R	
COMODO RSA Certification Au...	COMODO RSA Certification Auth...	1/18/2038	Client Authenticati...	Setigo (formerly C...	R	
COMODO RSA Certification Au...	COMODO RSA Certification Auth...	1/18/2038	<All>	<None>	R	
COMODO RSA Code Signing CA	COMODO RSA Certification Auth...	5/8/2028	Code Signing	<None>	R	
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timesta...	R	
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Client Authenticati...	DigiCert	R	
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	<All>	<None>	R	
DigiCert CS RSA4096 Root G5	DigiCert CS RSA4096 Root G5	1/14/2046	Code Signing, Time...	DigiCert CS RSA409...	R	
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authenticati...	DigiCert	R	
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	<All>	<None>	R	
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authenticati...	DigiCert Global Roo...	R	
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	<All>	<None>	R	
DigiCert Global Root G3	DigiCert Global Root G3	1/15/2038	Client Authenticati...	DigiCert Global Roo...	R	
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	11/9/2031	Client Authenticati...	DigiCert	R	
DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authenticati...	DigiCert Trusted Ro...	R	
DLA Forcepoint CA	DLA Forcepoint CA	6/13/2038	<All>	<None>	R	
DLA Root CA	DLA Root CA	5/31/2025	<All>	<None>	R	
DLA Root CA	DLA Root CA	5/31/2025	<All>	<None>	R	
DLA Root CA 2	DLA Root CA 2	2/8/2033	<All>	<None>	R	
DLA Root CA 2	DLA Root CA 2	2/8/2033	<All>	<None>	R	
DLA SCVP Responder 7	DLA SCVP Responder 7	7/13/2024	Server Authenticati...	<None>	R	
DLA SCVP Responder 8	DLA SCVP Responder 8	4/3/2029	Server Authenticati...	<None>	R	
DLAEntCA	DLA Root CA	5/9/2018	<All>	<None>	R	Subordinate C...
DoD Root CA 2	DoD Root CA 2	12/5/2029	<All>	<None>	R	
DoD Root CA 3	DoD Root CA 3	12/30/2029	<All>	<None>	R	
DoD Root CA 3	DoD Root CA 3	12/30/2029	<All>	<None>	R	
DoD Root CA 4	DoD Root CA 4	7/25/2032	<All>	<None>	R	
DoD Root CA 4	DoD Root CA 4	7/25/2032	<All>	<None>	R	
DoD Root CA 5	DoD Root CA 5	6/14/2041	<All>	<None>	R	

Trusted Root Certification Authorities store contains 133 certificates.

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

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
AddTrust External CA Root	Microsoft Code Verification Root	8/15/2023	Code Signing	<None>	R	
AFNOAPPS LTMA CA-1	AF LTMA Root CA	12/11/2026	<All>	<None>	R	Subordinate C...
COMODO RSA Code Signing CA	COMODO RSA Certification Auth...	5/8/2028	Code Signing	<None>	R	
DigiCert Global G2 TLS RSA SHA256 2020 CA1	DigiCert Global Root G2	3/29/2031	Server Authenticati...	<None>	R	
DigiCert SHA2 Assured ID Timestamping CA	DigiCert Assured ID Root CA	1/7/2031	Time Stamping	<None>	R	
DLA Enterprise CA 5	DLA Root CA 2	5/3/2026	<All>	<None>	R	Subordinate C...
DLA Enterprise CA 5	DLA Root CA 2	5/3/2026	<All>	<None>	R	Subordinate C...
DLA Enterprise CA 6	DLA Root CA 2	5/25/2027	<All>	<None>	R	Subordinate C...
DLA Enterprise CA 6	DLA Root CA 2	5/25/2027	<All>	<None>	R	Subordinate C...
DLA Root CA	DLA Root CA	5/31/2025	<All>	<None>	R	
DLA Root CA 2	DLA Root CA 2	2/8/2033	<All>	<None>	R	
DOD DERILITY CA-1	DoD Root CA 3	1/20/2027	<All>	<None>	R	
DOD DERILITY CA-1	DoD Root CA 3	1/20/2027	<All>	<None>	R	
DOD DERILITY CA-3	DoD Root CA 6	9/25/2029	<All>	<None>	R	
DOD DERILITY CA-3	DoD Root CA 6	9/25/2029	<All>	<None>	R	
DOD DERILITY CA-4	DoD Root CA 6	9/25/2029	<All>	<None>	R	
DOD DERILITY CA-4	DoD Root CA 6	9/25/2029	<All>	<None>	R	
DOD DERILITY CA-5	DoD Root CA 6	1/23/2031	<All>	<None>	R	
DOD DERILITY CA-6	DoD Root CA 6	1/23/2031	<All>	<None>	R	
DOD EMAIL CA-59	DoD Root CA 3	4/2/2025	<All>	<None>	R	
DOD EMAIL CA-62	DoD Root CA 3	6/9/2027	<All>	<None>	R	
DOD EMAIL CA-62	DoD Root CA 3	6/9/2027	<All>	<None>	R	
DOD EMAIL CA-63	DoD Root CA 3	6/2/2027	<All>	<None>	R	
DOD EMAIL CA-63	DoD Root CA 3	6/2/2027	<All>	<None>	R	
DOD EMAIL CA-64	DoD Root CA 3	6/2/2027	<All>	<None>	R	
DOD EMAIL CA-64	DoD Root CA 3	6/2/2027	<All>	<None>	R	
DOD EMAIL CA-65	DoD Root CA 3	6/9/2027	<All>	<None>	R	
DOD EMAIL CA-65	DoD Root CA 3	6/9/2027	<All>	<None>	R	