

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.

Name	Date modified	Туре	Size
\sim 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 >.

🕼 InstallRoot Setup	\times
InstallRoot Features	
Select the features you wish to install.	
Graphical Interface	
Command-Line Tool	
	< Back Next >

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

🕼 InstallRoot Setup	×
Begin installation of Instal	IRoot
Click Install to begin the installation. If yo click Back. Close the window to exit the w	u want to review or change any of your installation settings, izard.
	< Back Instal

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**.

🖟 InstallRo	ot Setup		×
	Installation Progress	\triangleright	
	Creating shortcuts		
	Installing InstallRoot		

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.

	×
DoD, ECA, JITC, WCF: Performed an online query and found there are no new TAMP messages to download.	

13. Click Install Certificates.

🎓 InstallRoot 5.5	-	×
Home Store Group Certificate Help		
Install Online Preferences Save Certificates Update Settings		
Action Application		
Computer Microsoft Local Computer		
✓ Install DoD Certificates		 👷 👻
× Install ECA Certificates 🥹		
× Install JITC Certificates 💿		 👷 👻
× Install WCF 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.

Target Certificate Store	Adds	Deletes
Microsoft Local Computer	0	0 of 10
Subject: DOD EMAIL CA-41; Issuer: DoD Root CA 3: Insufficient privileges		
Subject: DOD EMAIL CA-42; Issuer: DoD Root CA 3: Insufficient privileges		
Subject: DOD EMAIL CA-43; Issuer: DoD Root CA 3: Insufficient privileges		
Subject: DOD EMAIL CA-44; Issuer: DoD Root CA 3: Insufficient privileges		
Subject: DOD ID CA-41; Issuer: DoD Root CA 3: Insufficient privileges		
Subject: DOD ID CA-42; Issuer: DoD Root CA 3: Insufficient privileges		
Subject: DOD ID CA-43; Issuer: DoD Root CA 3: Insufficient privileges		
Subject: DOD ID CA-44; Issuer: DoD Root CA 3: Insufficient privileges		
Subject: DOD ID SW CA-37; Issuer: DoD Root CA 3: Insufficient privileges		
Subject: DOD ID SW CA-38: Issuer: DoD Root CA 3: Insufficient privileges		

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

DigiCert Global Root G2 Download PEM Download DER/CRT	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:CB: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:CB:5F Demo Sites for Root: Active Certificate expired revoked
DigiCert Global G2 TLS RSA SHA256 2020 CA1 Download PEM Download DER/CRT	Issuer: DigiCert Global Root G2 Valid until: 29/Mar/2031 Serial #: 00:F5:B0:06:28:56:02:F4:7A:88:50:20:23:00:F0:66 SHA1 Fingerprint: 18:51:1A:8E:AD:59:06:0E:20:70:77:00:8F:0E:00:43:81:38:26:12 SHA256 Fingerprint: 08:02:5F:9F:06:5F:0F:09:58:30:A8:00:78:67:89:A5:87:85:27:79:73:95:79:17:46:3F:08:13:D0:86:25:A9

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



20. Choose "Local Machine"

🔶 🛭 🐓 Certificate Import Wizard

Welcome to the Certific	ate Import Wizard
This wizard helps you copy certificate lists from your disk to a certificate sto	s, certificate trust lists, and certificate revocation re.
A certificate, which is issued by a cert and contains information used to prot connections. A certificate store is the	tification authority, is a confirmation of your identity tect data or to establish secure network : system area where certificates are kept.
Store Location	
O Current User	
O Local Machine	
To continue, click Next.	
	Vext Cancel

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

Х

Certificate Store Certificate stores are system areas where certificates are kept. Mindows can automatically select a certificate store, or you can specify a location for the certificate. Automatically select the certificate store based on the type of certificate Place all certificates in the following store Certificate store: Trusted Root Certification Authorities Browse	🖗 Certificate Import Wizard	
Windows can automatically select a certificate store, or you can specify a location for the certificate. Automatically select the certificate store based on the type of certificate Place all certificates in the following store Certificate store: Trusted Root Certification Authorities Browse	Certificate Store Certificate stores are system areas where certificates are kept.	
Automatically select the certificate store based on the type of certificate Place all certificates in the following store Certificate store: Trusted Root Certification Authorities Browse	Windows can automatically select a certificate store, or you can specify a location for the certificate.	
Place all certificates in the following store Certificate store: Trusted Root Certification Authorities Browse	O Automatically select the certificate store based on the type of certificate	
Certificate store: Trusted Root Certification Authorities Browse	O Place all certificates in the following store	
Trusted Root Cerbfication Authorities Browse	Certificate store:	
	Trusted Root Certification Authorities Browse	

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 Com	puter\Trusted Root Certification Autho	rities\Certificates]					- (×
File Action View Help								
🗢 🄿 🖄 💼 🖬 💼 🔒 🛽	? 📷							
Certificates - Local Computer Personal Certificates Certificates Certificates Certificates Certificates Certificates Computer Publishers Curricated Publishers Curricated Publishers Curricated People Cient Authentication Issuers	Issued To COMODO ECC Certification Au COMODO RSA Certification Au COMODO RSA Certification Au COMODO RSA Cede Signing CA Copyright (c) 1997 Microsoft C DigiCert Assured ID Root CA DigiCert Assured ID Root CA DigiCert CS RSA4096 Root G5 DigiCert CS RSA4096 Root G5	Issued By COMODO ECC Certification Auth COMODO RSA Certification Auth COMODO RSA Certification Auth COMODO RSA Certification Auth Copyright (c) 1997 Microsoft Corp. DigiCert Assured ID Root CA DigiCert SRSA4096 Root GS DigiCert GIobal Root CA	Expiration Date 1/18/2038 1/18/2038 1/18/2038 5/8/2028 12/30/1999 11/9/2031 11/9/2031 1/14/2046 11/9/2031	Intended Purposes Client Authenticati Client Authenticati Cale Signing Time Stamping Client Authenticati Cale Signing, Time Client Authenticati	Friendly Name Sectigo (formerly C Sectigo (formerly C < None> Microsoft Timesta DigiCert < None> DigiCert CS RSA409 DigiCert	Status R R R R R R R R R R	Certificate Tem	
> Preview Build Roots > Preview Build Roots	DigiCert Global Root CA	DigiCert Global Root CA DigiCert Global Root G2	11/9/2031 1/15/2038	<all> Client Authenticati</all>	<none> DigiCert Global Roo</none>	R		
AD Token Issuer CanaryCertStore EIM Certification Authorities	DigiCert Global Root G2 DigiCert Global Root G3 DigiCert High Assurance EV Ro	DigiCert Global Root G2 DigiCert Global Root G3 DigiCert High Assurance EV Root	1/15/2038 1/15/2038 11/9/2031	<all> Client Authenticati Client Authenticati</all>	<none> DigiCert Global Roo DigiCert</none>	R R R		
DisctorCertStore OEM eSIM Certification Auth OEM esim Trusted Roots	DigiCert Trusted Root G4 DLA Forcepoint CA DLA Root CA	DigiCert Trusted Root G4 DLA Forcepoint CA DLA Root CA	1/15/2038 6/13/2038 5/31/2025	Client Authenticati <all> <all></all></all>	DigiCert Trusted Ro <none> <none></none></none>	R R R		
PolicyCertStore CertStore Certificate Enrollment Reque:	DLA Root CA DLA Root CA 2 DLA Root CA 2	DLA Root CA DLA Root CA 2 DLA Root CA 2	5/31/2025 2/8/2033 2/8/2033	<all> <all> <all></all></all></all>	<none> <none> <none></none></none></none>	R R R		
Smart Card Trusted Roots SMS Trusted Packaged App Install:	DLA SCVP Responder 7	DLA SCVP Responder 7 DLA SCVP Responder 8 DLA Root CA DoD Root CA 2	4/3/2029 5/9/2018 12/5/2029	Server Authenticati <all></all>	<none> <none> <none></none></none></none>	R R R	Subordinate C	
Image: Second Seco	DoD Root CA 3 DoD Root CA 3	DoD Root CA 3 DoD Root CA 3 DoD Root CA 3	12/30/2029 12/30/2029 7/25/2032	<all></all>	<none></none>	R R		
WindowsServerUpdateService	DoD Root CA 4	DoD Root CA 4 DoD Root CA 5	7/25/2032 6/14/2041	<all> <all></all></all>	<none></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

🙀 Certificates - Local Computer	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem
> 🧰 Personal	AddTrust External CA Root	Microsoft Code Verification Root	8/15/2023	Code Signing	<none></none>	R	
> Trusted Root Certification Authorities	AFNOAPPS LTMA CA-1	AF LTMA Root CA	12/1/2026	<all></all>	<none></none>	R	Subordinate C
> 📔 Enterprise Trust	COMODO RSA Code Signing CA	COMODO RSA Certification Auth	5/8/2028	Code Signing	<none></none>	R	
 Intermediate Certification Authorities 	DigiCert Global G2 TLS RSA SHA256 2020 CA1	DigiCert Global Root G2	3/29/2031	Server Authenticati	<none></none>	R	
Certificate Revocation List	DigiCert SHA2 Assured ID Timestamping CA	DigiCert Assured ID Root CA	1/7/2031	Time Stamping	<none></none>	R	
Certificates	DLA Enterprise CA 5	DLA Root CA 2	5/3/2026	<all></all>	<none></none>	R	Subordinate C.,
> Irusted Publishers	DIA Enterprise CA 5	DLA Boot CA 2	5/3/2026	< 411>	<none></none>	R	Subordinate C
> Untrusted Certificates	DIA Enterprise CA 6	DLA Boot CA 2	5/25/2027	< 411>	<none></none>	R	Subordinate C
> Initia-Party Root Certification Authorities	DIA Enterprise CA 6	DIA Root CA 2	5/25/2027	< All>	<none></none>	R	Subordinate C
Client Authentication Issuers	DIA Boot CA	DIA Root CA	5/31/2025	<all></all>	<none></none>	R	
Preview Build Roots	DIA Root CA 2	DLA Root CA 2	2/8/2033	<all></all>	<none></none>	R	
> Test Roots	DOD DERILITY CA-1	DoD Root CA 3	1/20/2027	<all></all>	<none></none>	R	
> AAD Token Issuer	DOD DERILITY CA-1	DoD Root CA 3	1/20/2027	<all></all>	<none></none>	R	
> CanaryCertStore		DoD Root CA 6	9/25/2029	< All>	<none></none>	R	
> eSIM Certification Authorities		DoD Root CA 6	9/25/2029	< All>	<none></none>	R	
> injectorCertStore		DoD Root CA 6	9/25/2029	Alls	(None)	R	
> CEM eSIM Certification Authorities		DoD Root CA 6	9/25/2029	< Alls	(None)	R	
> 🧾 Passpoint Trusted Roots		DoD Root CA 6	1/23/2031	< Alla	(None)	R	
> 🧮 PolicyCertStore		DoD Root CA 6	1/22/2021	Alls	(None)	P	
> 🧮 Remote Desktop		DoD Root CA 3	4/2/2025	Alls	(None)	P	
> Certificate Enrollment Requests	DOD EMAIL CA-62	DoD Root CA 3	6/9/2027	< All>	<none></none>	R	
> In Runtime_Transport_Store_D2E68232-6F4D-		DoD Root CA 3	6/0/2027	Alls	None	P	
> Smart Card Trusted Roots		DoD Root CA 3	6/2/2027	< Alls	(None)	R	
> 📫 SMS		DoD Root CA 3	6/2/2027	<all></all>	<none></none>	P	
> Trusted Packaged App Installation Authori		DoD Root CA 2	6/2/2027	Alls	<none></none>	P	
> Trusted Devices		DoD Root CA 3	6/2/2027	<au></au>	<none></none>	P	
> Windows Azure Environment		DeD Root CA 3	6/0/2027	SAU2	<nere></nere>	R. D.	
> Windows Live ID Token Issuer		DeD Root CA 3	6/0/2027	Alls	<nene></nene>	D	
> WindowsServerUpdateServices		D-D R+ CA 5	5/15/2027	SAU2	<none></none>		