

Guide to Installing Certificates Java and .Net

Guide to Downloading and Installing DigiCert Certificates

The following steps should be taken to download the new certificates:

Download the new Intermediate Certificate

- 2 | Download the new DigiCert Intermediate Certificate
- 3 | Save the file with the name intermediate.pem. Make a note of the location of the file for future reference. For example, c:\windows\temp

Download the new Root Certificate

- 1 Next, <u>download</u> the root certificate
- 2 | Save the file with the name root.pem. Make a note of the location of the file for future reference. For example, c:\windows\temp

Guide to Installing GeoTrust Certificates for Java Applications and Utilities

To import the certificate files for Java applications and utilities.

- **1** | Find where Java is installed.
 - (a) If you already know where java is installed, you can ignore the next steps and skip to step 2.
 - (b) On a Unix system, you can run one of these commands "which java", "echo \$JAVA_HOME" or "locate java".
 - (c) On a Windows system, you can run the "echo %JAVA HOME%" command.
 - (d) For either of these, make a note of the path to the Java installation.
- 2 Once you have the path to the Java installation, run the following commands to install the certificates:

cd <path_to_java_from_step_1>

cd bin

keytool -import -alias GeoTrustTLSRSACAG1 -trustcacerts -file
<path_to_intermediate.pem> -keystore
<path_to_java_from_step_1>\jre\lib\security\cacerts

Note: for unix systems you may need to execute this as ./keytool

keytool -import -alias DigiCertGlobalRootG2 -trustcacerts -file <path_to_root.pem> - keystore <path_to_java_from_step_1>\jre\lib\security\cacerts



Note: For both of these commands, you will be prompted to enter the keystore password: enter your configured keystore password (the default is 'changeit')

Note: If you see an error "already exists," this means you already have the certificates, and can skip that

Guide to Installing DigiCert Certificates for .NET Applications

To import the certificate files for .NET applications.

1 | Click Start, click Run, type certmgr.msc, and then click OK.

Note: You may need administrative permissions to open certificate manager in Microsoft Management Console snap-in.

2 | Expand Certificates (local computer), expand Trusted Root Certification Authorities and then click Certificates, shown in Figure 3.

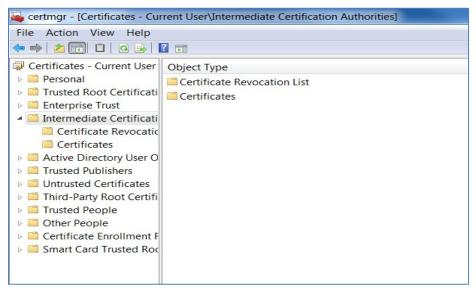


Figure 3 - Intermediate Certificate Store Location

3 | Confirm the intermediate certificate is not already listed – DigiCert SHA2

"pjm"

File Action View Help		
Þ 🔿 📶 🦨 🛍 🗙 🗐 🗟 🖬		
 Certificates - Current User Personal Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Certificate Revocation List Certificates Active Directory User Object Trusted Publishers Untrusted Certificates Certificate Trust List Certificates Trusted People Client Authentication Issuers Other People AdobeCertStore ISG Trust Local NonRemovable Certificates McAfee Trust Certificate Enrollment Requests Smart Card Trusted Roots 	Issued To COMODO RSA Code Signing CA DigiCert SHA2 Secure Server CA DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 EUS-STM-KEYID-FB17D70D734870E919C4E8E603975E664E Microsoft Azure RSA TLS Issuing CA 03 Microsoft Azure RSA TLS Issuing CA 04 Microsoft Azure RSA TLS Issuing CA 08 Microsoft TPM Root Certificate Authority 2014 Microsoft Windows Hardware Compatibility PJM Issuing CA v2 PJM Root CA 2023 PJM Root CA 2023 PJM Windows Issuing CA PJM Windows Issuing CA 2023 PJM Windows Issuing CA 2023 PJM Windows Issuing CA 2023 Signational State Cartificate Code Signing CA Symantec Class 3 SHA256 Code Signing CA	Issued By COMODO RSA Certification Auth DigiCert Global Root CA DigiCert Trusted Root G4 Microsoft TPM Root Certificate A DigiCert Global Root G2 DigiCert Global Root G2 DigiCert Global Root G2 Microsoft TPM Root Certificate A Microsoft Root Authority PJM Root CA v2 PJM Root CA 2023 PJM Root CA 2023 PJM Root CA 2023 PJM Root CA 2023 DigiCert Global Root G2 Root Agency VeriSign Class 3 Public Primary Ce

Figure 4 - Confirm GeoTrust Intermediate Certificate

- 4 | If not listed, expand certificates (local computer), expand Intermediate Certification Authorities right- click Certificates, click All Tasks, and then click Import.
- **5** | **Import** the intermediate certificate.
 - (a) In the **Certificate Import Wizard** dialog box, figure 5, click **Next**.



1	🤹 certmg	Certificate Import Wizard	×
	File Act File Act Certific Pers Certific Certif		<text><text><text><text></text></text></text></text>
			< Back Next > Cancel

Figure 5 - Certificate Import Wizard

(b) In the **File name** box (figure 6), give the path of the intermediate certificate authority file downloaded in the first section of this document. For example, c:\windows\temp\intermediate.pem

Ce	ertificate Import Wizard		
-	File to Import Specify the file you want to import.		
	File name:		
	Note: More than one certificate can be stored in a single file in the following formats:		
Personal Information Exchange- PKCS #12 (.PFX,.P12)			
	Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)		
	Microsoft Serialized Certificate Store (.SST)		
-	< Back Next > Cancel		

Figure 6 - Import File

- 6 | Click **Next** two times.
- 7 | Click **Finish**, and then click **OK**. You should see a message appear 'The import was successful'.



Import the Root Certificate

- 8 | Expand Certificates (local computer), expand Trusted Root Certification Authorities, and then click Certificates.
 - (a) In the right pane, confirm that the certificate for 'DigiCert Global Root CA' is not listed.
 - (b) If not listed, **import** the root certificate.
 - (c) Expand Certificates (local computer), right-click Trusted Root Certification Authorities, click All Tasks, and then click Import.
- 9 | Import the root certificate
 - (a) In the Certificate Import Wizard dialog box, figure 7, click Next.

ſ	ᡖ certmg	Certificate Import Wizard	×
	File Act File Act Certific Certific File Pers File Certific File Certific		<text><text><text><text></text></text></text></text>
-	A.M.		< Back Next > Cancel

Figure 7 - Certificate Import Wizard

(b) In the File name box (figure 8), give the path of the root certificate authority file downloaded in the first section of this document. For example, c:\windows\temp\root.pem



File	e to Import
	Specify the file you want to import.
	File name:
	Browse
	Note: More than one certificate can be stored in a single file in the following formats
	Personal Information Exchange- PKCS #12 (.PFX,.P12)
	Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
	Microsoft Serialized Certificate Store (.SST)
eai	rn more about <u>certificate file formats</u>
	< Back Next > Cance

Figure 8 - Import File

- **10** | Click **Next** two times.
- **11** | Click **Finish**, and then click **OK**. You should see a message appear 'The import was successful'.