

A Trusted Advisor of Security Solutions and Services

#TrustedPKIAdvisor

Google App Engine: SSL Certificate Installation

https://www.acmetek.com



WHITE PAPER

Google App Engine (often referred to as **GAE** or only **App Engine**) is a **Platform as a Service** and **cloud computing** platform for developing and hosting **web applications** in Google-managed **data centers**. Applications are **sandboxed** and run across multiple servers. App Engine offers automatic scaling for web applications—as the number of requests increases for an application, App Engine automatically allocates more resources for the web application to handle the additional demand.

SSL Installation Steps:

- Import your SSL Certificate to your Windows server or workstation using the DigiCert[®] Certificate Utility for Windows.
- Export the SSL Certificate in Apache compatible .pem format (separate .key and .crt files) using the DigiCert[®] Certificate Utility for Windows
- Append the Intermediate Certificate to the end of the SSL Certificate file.
- Upload and configure your SSL Certificate using the Google Admin console.

Importing an SSL Certificate Using the DigiCert Certificate Utility

After we validate and issue your SSL Certificate, you can use the DigiCert[®] Certificate Utility for Windows to import the file to your Microsoft server or workstation.

- 1. On the server or workstation where you created the CSR, save the SSL Certificate .cer file (i.e. your_domain_com.cer) that DigiCert sent to you.
- 2. Run the DigiCert[®] Certificate Utility for Windows. Double-click **DigiCertUtil**.
- 3. In DigiCert Certificate Utility for Windows©, click SSL (gold lock) and click Import.



4. In the Certificate Import window, under File Name, click Browse to browse to the .cer (i.e. your_domain_com.cer) certificate file that DigiCert sent you, select the file, click Open, and then, click Next.

0	DigiCert Certificate Utility for Windows©
	Certificate Import
	This wizard will assist you with importing a certificate. Depending on the type of file you are importing you may be prompted for a password to decrypt the private key. File Name
	C:\certs\your_domain_com.cer Browse
-	
	< Back Next > Cancel

5. In the **Enter a new friendly name or you can accept the default** box, enter a friendly name for the certificate. The friendly name is not part of the certificate; instead, it is used to identify the certificate.

We recommend that you add DigiCert and the expiration date to the end of your friendly name, for example: yoursite-DigiCert-expirationDate. This information helps identify the issuer and expiration date for each certificate. It also helps distinguish multiple certificates with the same domain name.

0	DigiCert Certificate Utility for Windows©	×
Cert	ificate Import	
The follow the certif Name: Serial Nu Thumbpri Private K	wing certificate is ready to be imported. For more details of ficate press the View Certificate button. yoursite int: 8208519D 1D940FC2C76338D446D5A496ECEF34A3 Key: Search for an existing private key match on the computer]
Enter a n	new friendly name or you can accept the default:	
yourGoo	ogleApp-DigiCert-expirationDate	
Press the	e Finish button to import the certificate and search for a matching private key.	
-	< Back Finish Cancel	

6. Click Finish

Exporting a SSL Certificate in Apache Compatible .pem Format Using the DigiCert Certificate Utility

To make an SSL connection, your server needs two parts, a private key file and the certificate file. Apache (and many other server types) separate these two certificate parts into separate .key file and .crt files (both files are .pem formatted files).

- 1. Run the DigiCert[®] Certificate Utility for Windows. Double-click **DigiCertUtil**.
- 2. In **DigiCert Certificate Utility for Windows**©, click **SSL** (gold lock), select the SSL Certificate you want to export, and then, click **Export Certificate**.

		DigiCert Certifica	ate Utility for Wi	ndows© X
Gdig	icerť	CERTIFICATE UTILITY fo	r Windows®	\$ 1.800.896.7973 support@digicer.com Live Chat
-	SSL Certificates			Create CSR 🛧 Import C Refresh
	Issued To	Expire Date	Serial Number	Friendly Name Issuer
	yoursite	10-SEP-2014	08	DigiCert, Inc.
Tools				
Account				Export Certificate Test Key View Certificate
ersion 2.3.7				Close

3. In the **Certificate Export** wizard, select **Yes, export the private key**, select **key file (Apache compatible format)**, and then, click **Next**.

۵	DigiCert Certificate Utility for Windows©
Се	rtificate Export
This v certif You n a diff Do y	vizard will export a certificate and optionally its private key from the icate store to disk. nust select the private key option if you wish to install this certificate on erent computer. ou want to export the private key with this) <u>Y</u> es, export the private key ○ pfx file Indude all certificates in the certification path if possible () key file (Apache compatible format)) <u>N</u> o, do not export the private key
	< Back Next > Cancel

- 4. In the File name box, click ... to browse for and select the location and file name where you want to save the certificate .crt and .key files, and then, click Finish. This creates the following files that you will need to upload and configure using your Google Admin console.
 - Private Key: your_domain_com.key
 - Server Certificate: your_domain_com.crt
 - Intermediate Certificate: DigiCertCA.crt

Note: The .key and .crt files are in .pem format, they are just named with .key and .crt.

۵	DigiCert Certificate Utility for Windows©	×
C	ertificate Export	
En an En	ter the file name that you want to save the exported certificate to d press Finish to export the certificate. ter a file name for the exported File name	
	C:\Users\Support\yoursite.key	
-		
	< Back Finish	Cancel

5. After you receive the "Your certificate and key have been successfully exported" message, click **OK**.

Appending the Intermediate Certificate to Your SSL Certificate

SSL .pem files (concatenated certificate container files), are frequently required for certificate installations when multiple certificates are being imported as one file.

Because your DigiCert issued SSL Certificate (host certificate) requires an intermediate certificate (chained certificate), Google App Engine requires that append the intermediate certificate to the end of your SSL Certificate.

You can use a text editor or the command line to create your new SSL Certificate concatenated .pem file.

- Using a Text Editor to Create a .pem with the Server and Intermediate Certificates
- Using Command Line to Create a .pem with the Server and Intermediate Certificates

Using a Text Editor to Create a .pem with the Server and Intermediate Certificates

- 1. Open a text editor (such as Notepad or WordPad) and paste the entire body of each certificate into one text file in the following order:
 - a. The Primary Certificate your_domain_name.crt
 - b. The Intermediate Certificate DigiCertCA.crt
- Make sure to include the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- tags on each certificate.



3. The text file should look like this:

-----BEGIN CERTIFICATE-----

(Your Primary SSL certificate: your_domain_name.crt)

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

(Your Intermediate certificate: DigiCertCA.crt)

-----END CERTIFICATE-----

yoursite.crt - Notepad	_ 0	x
File Edit Format View Help		
BEGIN CERTIFICATEMIIB0TCCATqgAwIBAgIQR/40WrBxs6FHqRMZ1zRWWjANBgkqhkiG9w0BAQUFADAU <u>YOUr_domain_name.crt</u> MRIwEAYDVQQDEw1sb2NhbGhvc3QwdHcNMTMwNDESMDMyODA3WhcNMTgwNDE4MDAwUjAUWRIwEAYDVQQDEw1sb2NhbGhvc3QwgZ8wDQYJKoIThvcNAQ MIGJAoGBAMUKnjfSN+D/K1araRHfjDqr7dnOPBf0HiCNa7z4De8dfLSnyiLNJRpBLABZA/Az1U2VFF+zRgsIBddKzUWxyxPxE5kAeOUs6CNAygTaR8bVN vcMy73EgkcDn9qq8kvwE+ui0EyNyvKRBJaE8MTbF0xgScfWyzW/DAgMBAAGjJDA1MAsGA1UdDwQEAwIEsDATBgIVHSUEDDAKBggrBgFBQcDATANBgkqhk AAOBgQB0n5d+PYyYY3BqKESW+sK3VNhKybP3KMvOuIpusG/3f14VPEhXOH1rrK1rphG0Ep5hSumBEAHJekf1p251JMFB/SUVKfifq8WvdcrQgrG8JMJQEC g7554WmA4J4Caixy8WfT/xIjupQEDwnL0Dxa/QPOStqs8161dA==END CERTIFICATE	BBQADgY0A <jg+f9 d01<br="">iG9w0BAQUF 3I5ngvVXUq</jg+f9>	
BEGIN CERTIFICATEMIIGWDCCBUCgAwIBAgIQC18RTQNbF5EX0u/UA4w/OzANBgkqhkiG9w0BAQUFADBs		
MQswCQYDVQQGEwJVU2EVMBMGA1UEChMMRG1naUN1cnQgSW5jMRkwFwYDVQQLExB3d3cuZG1naWN1cnQuY29tMSswKQYDVQQDEyJEaWdqQ2VydCBIaWdoIE ZSBFViBSb290EINBMB4XDTAAMDQwHjEyMDAwMFoXDTJYMDQwHzAwMDAwMFowZjELMAkGA1UEBhMCVMXrTATBgHVBAoTDERp221DZXJ0IELVYzEZMEGGAL LmRp221jZXJ0LmNvbTEIMCMGA1UEAxMcRG1naUN1cnQgSG1naCBBc3N1cmFuY2UgQ0EtMzCCASIwQYJKoZINvcNAQEBBQADggEPADCCAQoCggEBAL9hCi (CPg+yLtYb4LDXBMUGMmdRWSQY1XtvCgFbsIYOBC6AUpEIc21ih1q08xB3RtNpcvKEZmBMcqeSZ6mdИ0w21PoF6tvD2Rw117XjZswFPPAAgyPhBkWBATac BUTuJMS6H+2MED65qPMV9Bx6MwkB66fmxCcabH4JnudSREoQ01Pkm7VDr6ictFuf1Eutko20tREqqjcYjDTCuNhcBoz4/y09NV7UFD5+gwGR1gMVvJTf48 zPw82W3tzPpLQ4zJ1Li1RyyQLY0Et+5+F/+07LJ7z20HktBHEyZNP469+npF4d32duXvsCAwEAaoCAvowggL2MA4GA1UdbwEB/wQEAwIBhjCCAcYGA1 ggGSMIIBtQYLYIZTMY9bAEDAATwggGkMDoGCCsGAQUFBwIBF1SodHRw018vd3d3LmRp221jZXJ0LmNvb59zc2vtY3BzLXJ1c69zaRVcnkuaHRtMIIBZA AgIwggFWH0IBUgBBAG4AeQAgAHUAcwB1ACAAbwBmACAAdABoAGAcwAgAEMA2QByAHQAaQBmAGkAYwBhAHQAZQAgAGMAbwBuAHMAdABpAHQAdQBBAGUAcA AGEAcgBBAHkAIABBACAcegB1AGUALAbQB1AGAAdAAgAHcAAABABAGMAAQWB1AHIAdAAAgAEMAUAAvAEMAUABTACAAYQBuAGQMIAB0AGaZQAgAF1AZQBSAHkAAQ AGEAcgBBAHkAIABBACAcegB1AGUALAbQB1AGAAdAAgAHcAAABABpAGMaAAgAGwAAQBHAGKAAQBABCAGAAQBAGAGAQBhAGIAAQBAACAAYQBUAGQATAB0AGgAZQAgAF1AZQBSAHkAAQ AGEAcgBBAHkAIABBACAcagB1AGUALAbQB1AGAAdAAgAHcAABABAGMAAAAgAGwAAQBHAGIAAQBACAAYQBUAGQAACAAYQBUAGQATAB0AGaZQAgAF1AZQBSAHkAAQ AGEAcgBBAHkAIABBACACAG2B1AGUADQB1AGAAAABAgAGAAAAgAGwAAQBCAGAKAAAAgAGwAAQBhAGIAAQBSACKAAMBSACAAYQBUAGQAACAAYQBUAGQAAGAATABAHTAZQ AGEAcgBBAAKALABBACACAGB1ABUADQB1AGAAABAGAAAABAGAWAAQGUAZgB1AHIAZQBUAGMAZQAUMBIGALUdewEB/wQIMAYBAF8CAQAwNAYIKwYBBQ MCQGCCsGAQUFBZABhhodHRw018vb2NzcCSsaWdpY2VydC5jb20wgV8GA1UHkSbr2CBNDBAOBGgPYGaHRRcDovL2NybDMV2GInaWN1cnQuY29tL0RpZ2 aEFzc3VYW5jUVWUm9vdENBLmNybDBAOBGPTYGaHR0cDovL2NybDQUZGInaWN1cnQU729tL0RpZ30GInaEFzc3VyW5jJUVWUm9vdENBLmNybD V060dRvw/S41WawTWGHI5/rpmc2HCXVUKL9GYNJYUSYS8xuRfDEIc0I3ucFbqL2jCwD7GNX9A61YaSXHJJ1IR0YXHpLvtF90NMeQvzHB+LGEhtCcAarf11 dF3XcZpCdF/ejUN83u1V7WkAywXgemFhM9EZTfkI7qA5xSU1tyvED7Ld8aW3DITE311NeXf1L/BXunwH10HBzVovV36GEEFdMR/X/KLCvzB8XSSq6PmuX2 Ib4p115eFdZCS	zc3VyYW5j IEC:MQd3d3 :QH17+NDdR :M7pxCUQD5 116617XaAs JdIASCAb0w IGAGCAIABQ IGAGCAIABQ JAQEEKDAm IDZXJ0SG1n \FBgNVHSME (GzjrpDq6X 30ws5rs0bY	

4. Save the combined file as your_domain_name.pem.

The SSL Certificate .pem file (your_domain_name.pem) is now ready to upload to the Google Admin console.

Using Command Line to create a .pem with the Server and Intermediate Certificates

- 1. Open the folder that contains the Primary Certificate your_domain_name.crt and the Intermediate Certificate – **DigiCertCA.crt**.
- 2. Hold down the **shift** key and right-click in the folder and then, select **Open command window here.**



3. In the Command line, type the following command:

type your_domain_name.crt DigiCertCA.crt > your_domain_name.pem

Note: Make sure to replace your_domain_name with the name of your Server Certificate.



4. To see your appended Server Certificate (your_domain_name.pem), type the following command:

type your_domain_name.pem

Note: Make sure to replace your_domain_name with the name of your Server Certificate.



5. The SSL Certificate .pem file (your_domain_name.pem) is now ready to upload to the Google Admin console.



Google App Engine: Uploading and Configuring Your SSL Certificate

To install your Google App Engine SSL Certificate, first, you need to upload the certificate to the Google Admin console. Then, you need to configure the certificate. Because every environment is different (for example your settings may be configured differently), you may need to consult your Google App Engine documentation. For more advanced configuration, you should consult the Google documentation.

Uploading Your Certificate and Private Key

1. Log into the Google Admin console as a Super Admin.



- 2. In the console, Click Security > (optional) Show more > SSL for Custom Domains.This link only appears if you have set up a subdomain.
- 3. Click Configure SSL certificate.

4. On the SSL Certificate Configuration page, in the New Certificate section, click Upload a new certificate.

New Certificate	It is now possible to use SSL on mysite.com. An SSL certificate and private key will need to be uploaded for SSL to be available for any custom URLs.	
	Upload a new certificate	

5. Under **PEM encoded X.509 certificate**, click **Choose File** to locate and select your_domain_ name.pem certificate file.

New Certificate	It is now possible to use SSL on appenginetest.com. An SSL certificate and private key will need to be uploaded for SSL to be available for any custom URLs. (2)
	PEM encoded X.509 certificate
	Choose File No file chosen
	Unencrypted PEM encoded RSA private key
	Choose File No file chosen
	Upload Cancel

6. Under **Unencrypted PEM encoded RSA private key**, click **Choose File** to locate and select your_domain_name.key private key file.

Note: The .key file that you received when you exported your SSL Certificate in Apache com patible format is a .pem formatted file.

7. After you have selected your certificate and private key, click **Upload**.

Configuring Your Certificate

After successfully uploading your certificate and key files, you can configure your SSL Certificate.

1. In the **Current state** section, in the **Serving mode** drop-down list, select a serving method.

The list only displays the available serving methods, which is determined by whether you have VIP, SNI, or VIP and SNI certificate slots. Note that the **SNI + VIP** option does not use a SNI certificate slot; instead, the certificate is assigned to the VIP that is listed.

Current state	Serving mode:	Not serving	Th
	CNAME to:		-1

For more information about serving modes, see the Google App Engine documentation.

2. In the Assigned URLs section do one of the following:

• Manually add each matching URL.

In the drop-down list select a matching URL and then, click Add.

• Add all matching URLs.

Click Assign all matching URLs.

Assigned URLs	No URLs assigned yet
	Y Add
	Assign all matching URLs Unassign all Replace certificate

- 3. For more information about matching URLs, see the Google App Engine documentation.
- To change the CNAME record for your assigned URLs to the CNAME provided in the CNAME to field, contact your DNS provider.

For more information about the **CNAME to** field, see the Google App Engine documentation.

- 5. When you are finished, at the bottom of the page, click **Save**.
- 6. Your SSL Certificate has now been successfully uploaded and configured.

We hope this guide helped you with this easy process. If you are unable to use these instructions, Acmetek recommends that you contact either the vendor of your software or the hosting organization that supports it.

ABOUT ACMETEK

"Acmetek is a Global Distributor and a Trusted Advisor of PKI /IoT & SSL Security Products and Managed Services Company."

<u>Acmetek Global Solutions, Inc.</u> is a privately held Digital Security Services Company serving USA & APAC clients in website security solutions since 2010. The firm specializes in providing insight and expertise to enterprises, SMBs, governments, and provides a full range of Security Products, SSL, PKI, IoT, Malware Identity Scanning's, Vulnerability Assessments, and Two-Factor Authentication.

Acmetek is a managed service partner of multi-brand technology solutions like CDW. We manage the Certificate Authority Practices of leading Website Security Brand, DigiCert (formerly known as Symantec). Over a decade of experience in the security industry empowered us to grow as an Authorized Distributor/ Platinum Partner for DigiCert and a leading provider of security solutions and services.

SSL Cert Free Trial | MPKI | Request a Call Back | SSL Support Desk

Our Web Security Solutions

SSL CERTIFICATES

MPKI SOLUTIONS



Domain Validation

Extended Validation

Activates HTTPS with a padlock. This SSL can issue in minutes.

Activates HTTPS with a padlock. It validates

the organization by providing the company

name before the domain name directly



Organization Validation

Activates HTTPS with a padlock. It validates an organization by providing a trust seal.



Code Signing Certificates

Protects users from downloading compromised software, prevents tampering, and provides the trusted assurance of authentication.



Email Certificates

on the browser.

Using an Email certificate for user authentication encrypts transmission and signs the message,delivering comprehensive benefits for the sender and receiver.



Device Certificate

Verify identity, encrypt communications, and secures all home networks for internet connected devices before and after manufacturing.

WIFI Certificates

Increases trust in public hotspots and protect user data.



Document Signing Certificates

Document signing certificates allow individuals, teams, and organizations to add an electronic, digital signature to a document in a variety of file formats to prove ownership.



MDM (Mobile Device Management)

Get a comprehensive look at mobile devices, master mobile email, and application rollout while protecting all data and devices.