Acmetek

A Trusted Advisor of Security Solutions and Services

#TrustedPKIAdvisor

# Google App Engine: SSL Certificate Installation

WHITE PAPER

https://www.acmetek.com

**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.

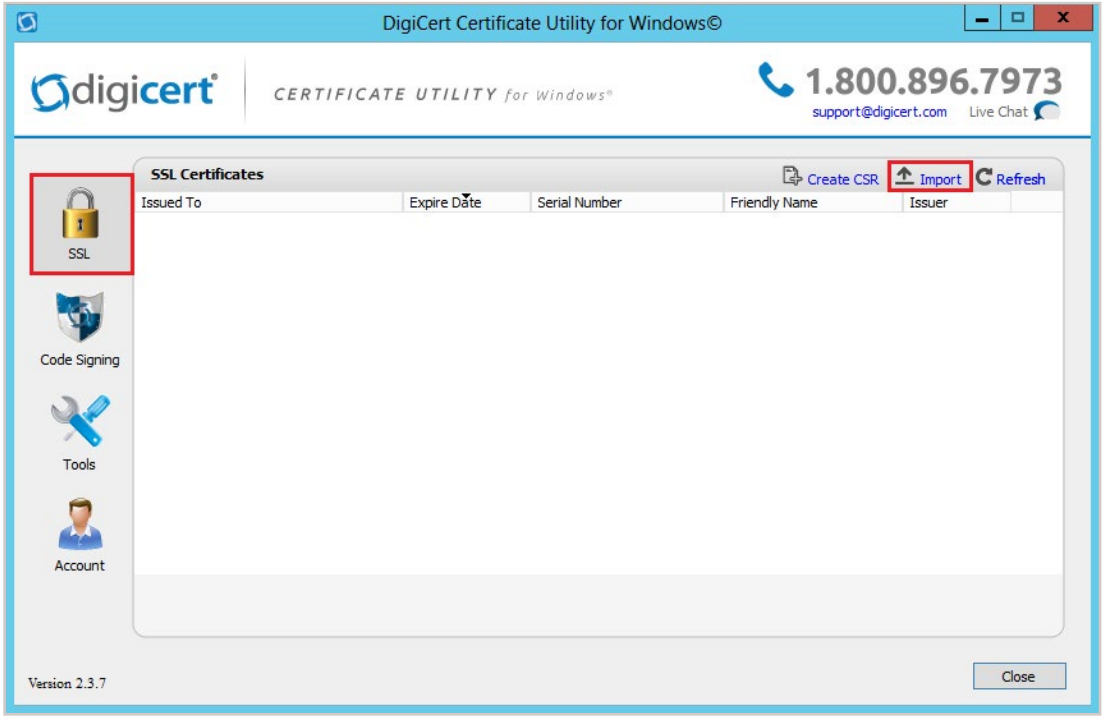
## SSL Installation Steps:

- 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.

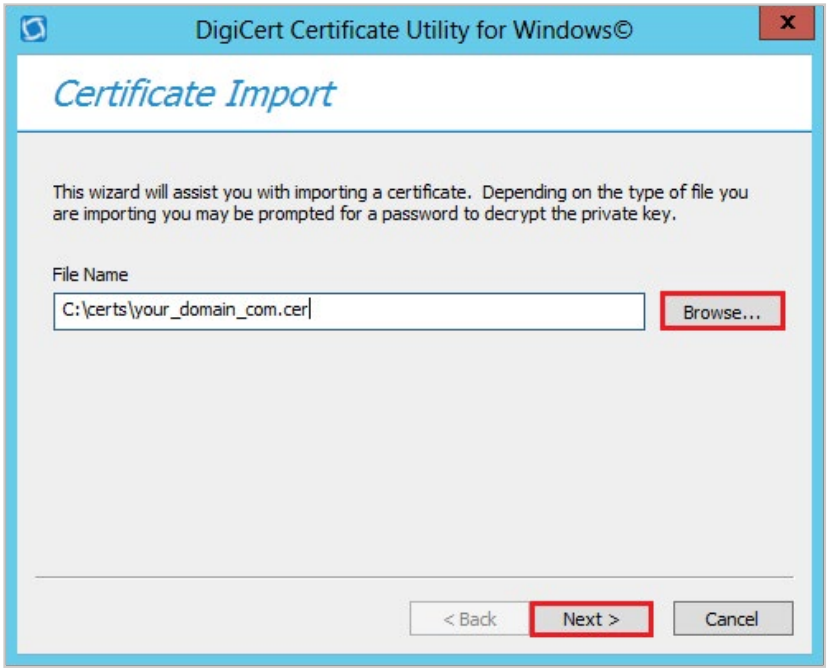
### Importing an SSL Certificate Using the DigiCert Certificate Utility

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**.

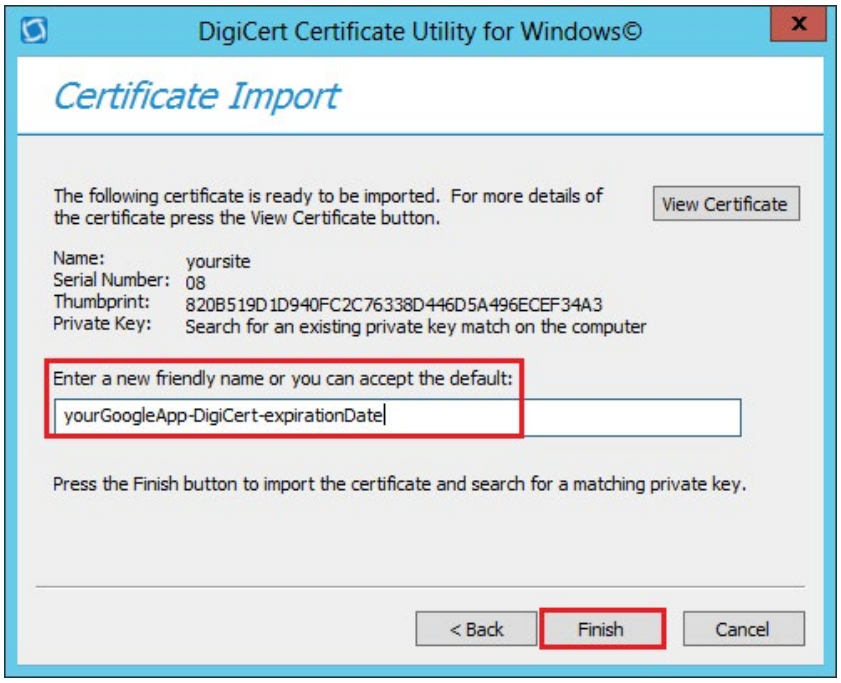


4. In the **Certificate Import** window, under **File Name**, click **Browse** to browse to the .cer (i.e. your_domain_com.cer) certificate file that DigiCert sent you, select the file, click **Open**, and then, click **Next.**




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.



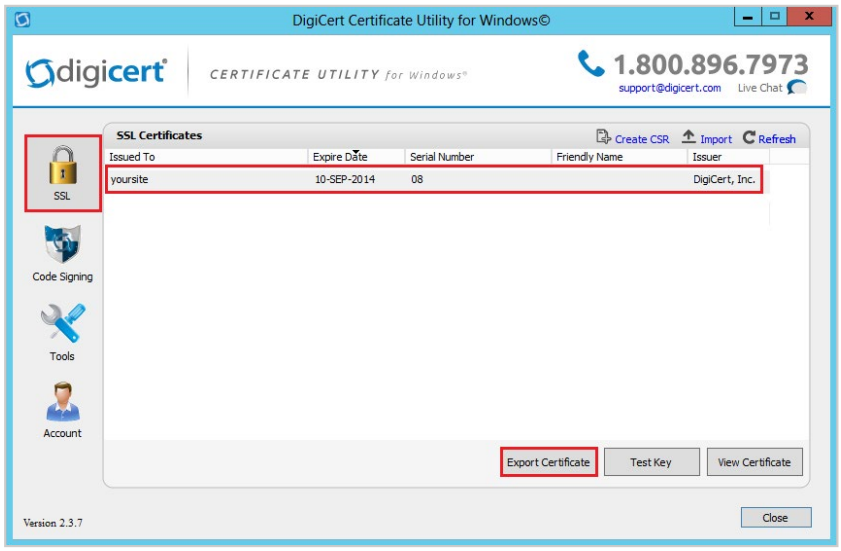
6. Click **Finish**

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

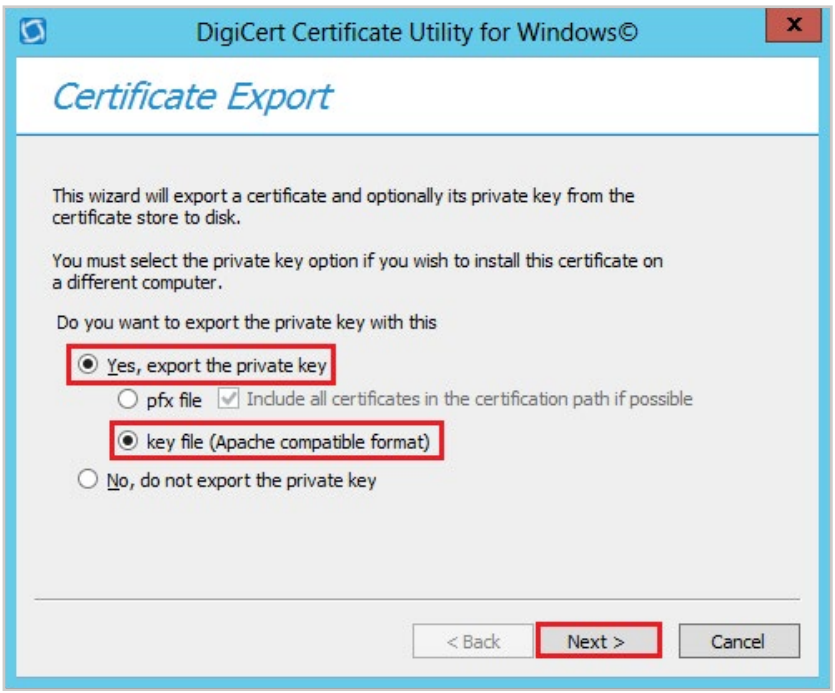
To make an SSL connection, your server needs two parts, a private key file and the certificate file. Apache (and many other server types) separate these two certificate parts into separate .key file and .crt files (both files are .pem formatted files).

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**.

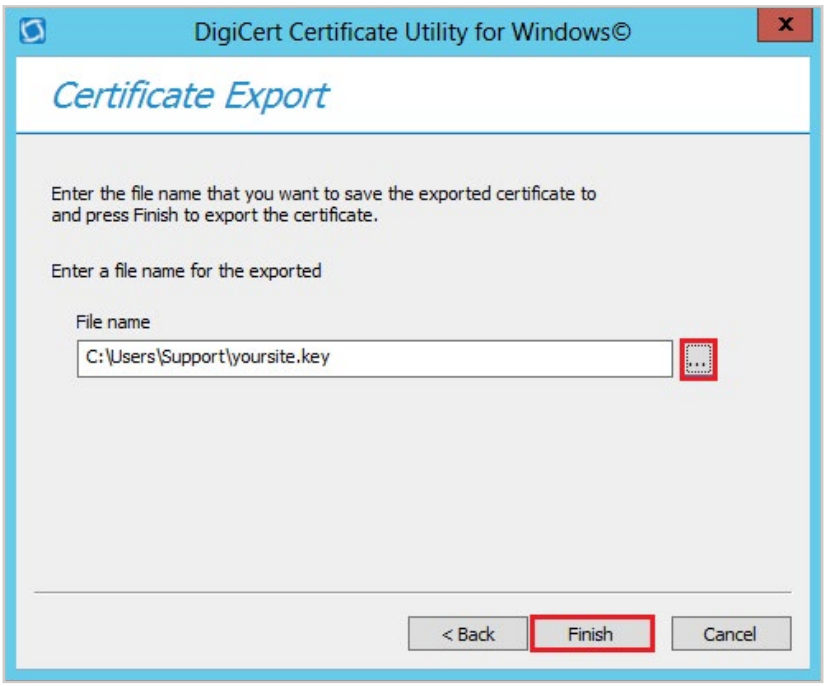



3. In the **Certificate Export** wizard, select **Yes, export the private key**, select **key file (Apache compatible format)**, and then, click **Next**.



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.




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.

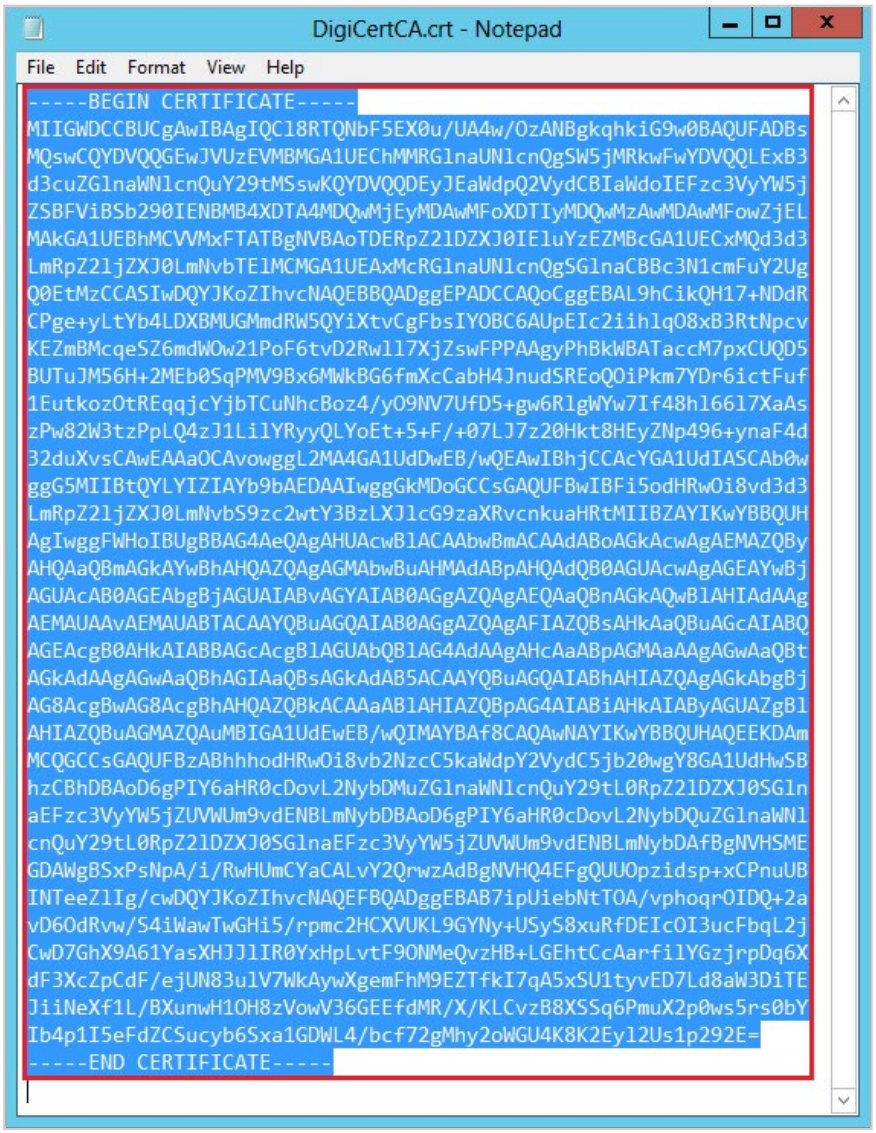
Because your DigiCert issued SSL Certificate (host certificate) requires an intermediate certificate (chained certificate), Google App Engine requires that append the intermediate certificate to the end of your SSL Certificate.

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**
2. 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)**

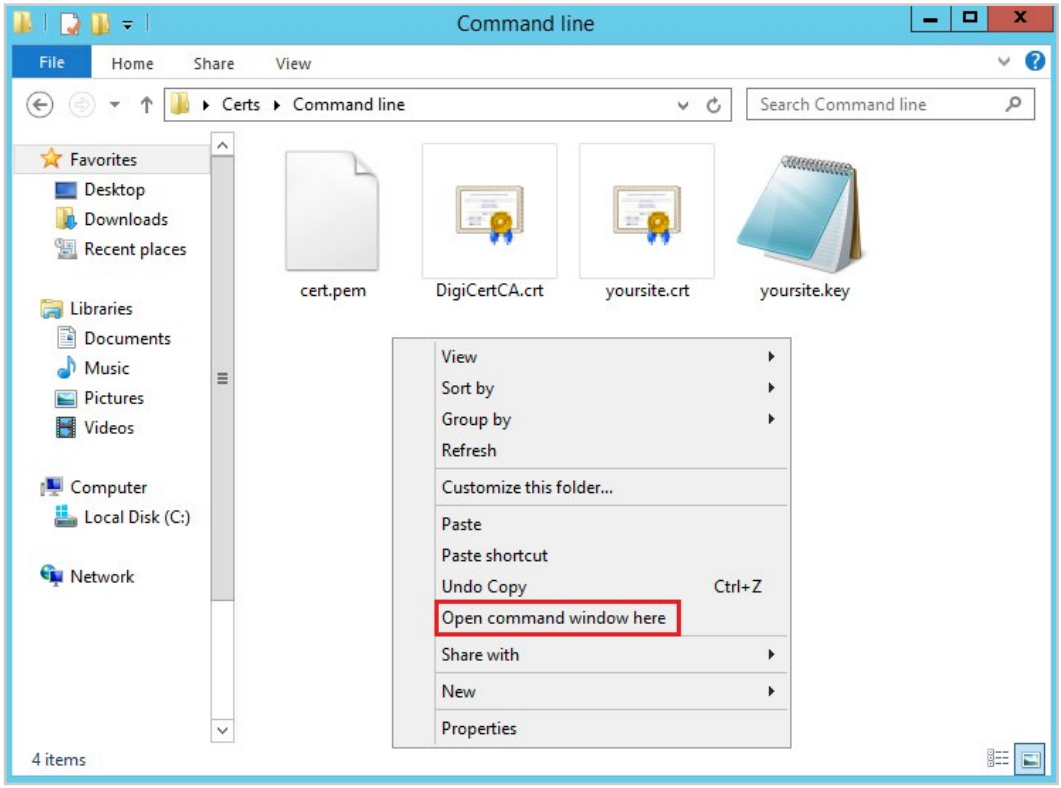
    **-----END CERTIFICATE-----**


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

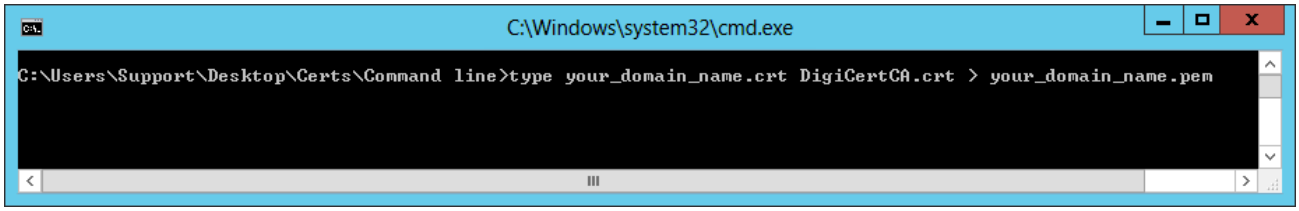
1. Open the folder that contains the Primary Certificate – your_domain_name.crt and the Intermediate Certificate – **DigiCertCA.crt**.
2. Hold down the **shift** key and right-click in the folder and then, select **Open command window here.**



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

   **type** your_domain_name.crt DigiCertCA.crt > your_domain_name.pem

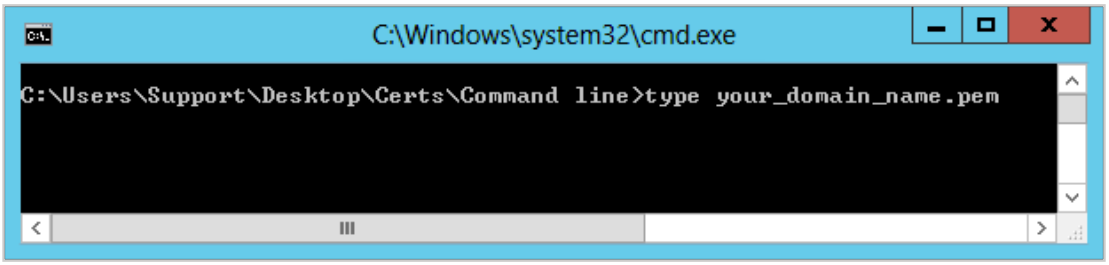
   **Note:** Make sure to replace your_domain_name with the name of your Server Certificate.




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.



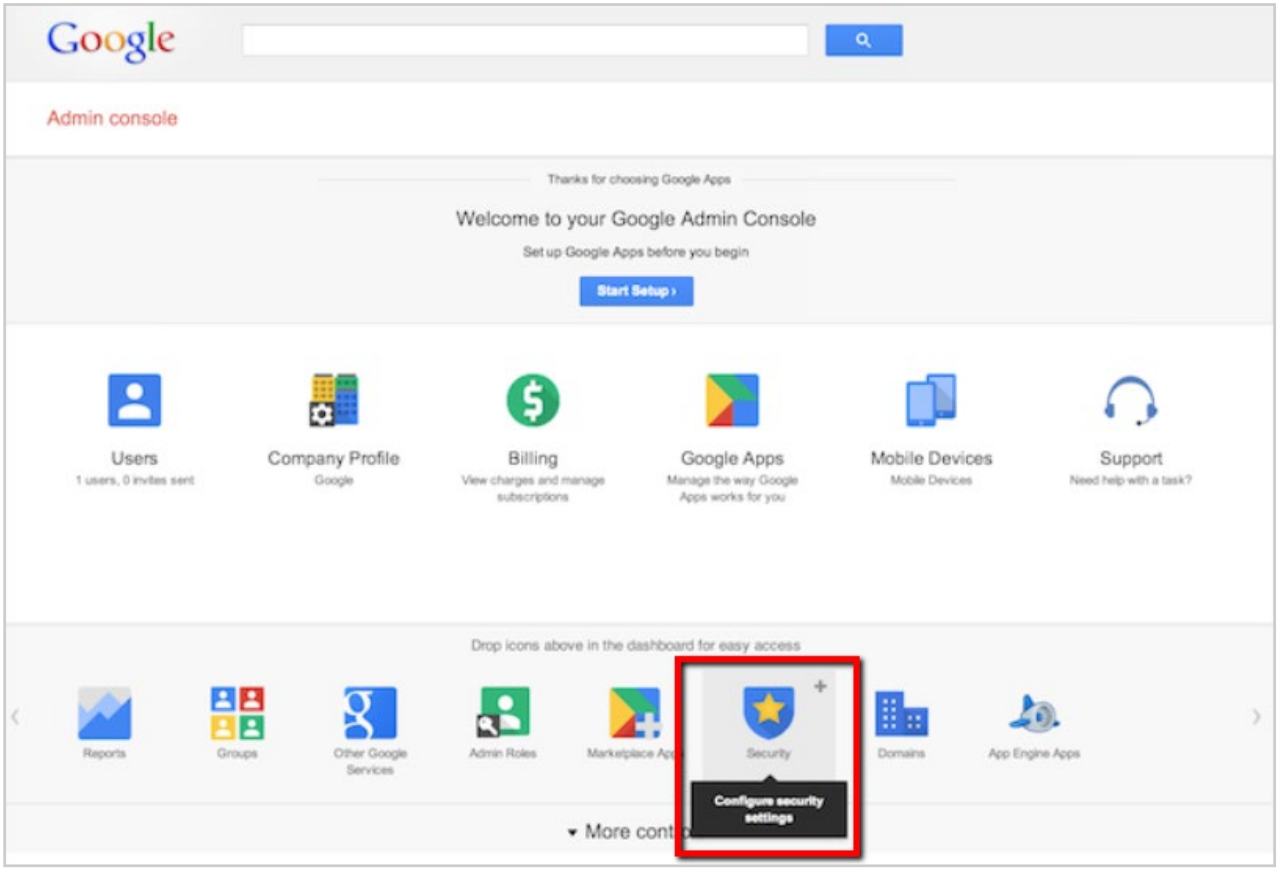

5. The SSL Certificate .pem file (your_domain_name.pem) is now ready to upload to the Google Admin console.

## 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

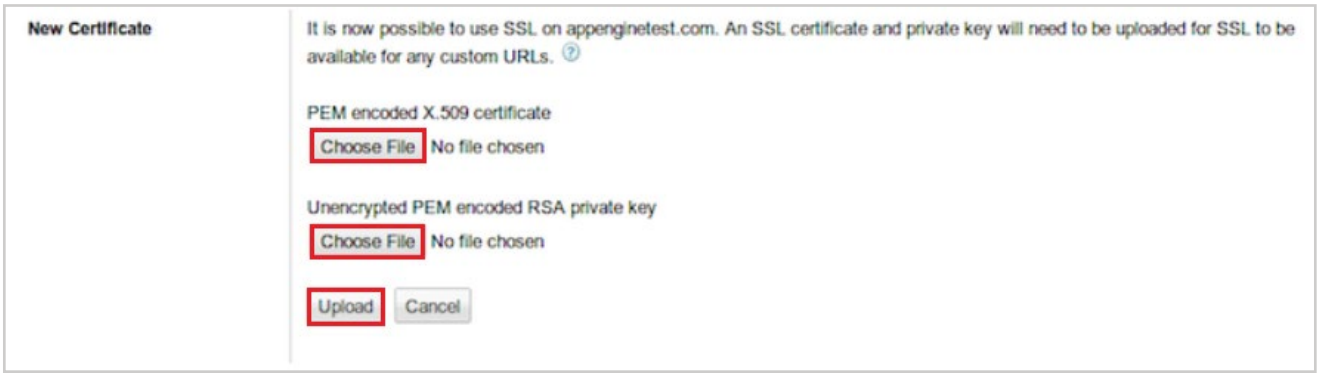
1. Log into the Google Admin console as a Super Admin.




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**.


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




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 compatible format is a .pem formatted file.

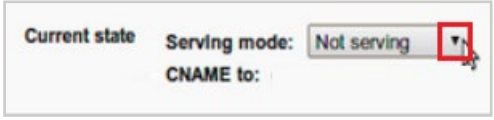
7. After you have selected your certificate and private key, click **Upload**.

### 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.




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**.


3. For more information about matching URLs, see the Google App Engine documentation.
4. 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.”**

Acmetek Global Solutions, Inc. 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

**Domain Validation**

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

**Organization Validation**

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

**Extended Validation**

Activates HTTPS with a padlock. It validates the organization by providing the company name before the domain name directly on the browser.

**Code Signing Certificates**

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

### MPKI SOLUTIONS

**Email Certificates**

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

**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.

**Device Certificate**

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

**MDM (Mobile Device Management)**

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

**WIFI Certificates**

Increases trust in public hotspots and protect user data.