**How to install an SSL Certificate on GlassFish?**

Tuesday, February 12th, 2019

In this guide, you’ll learn how to install an SSL Certificate on GlassFish. If you haven’t generated the CSR (Certificate Signing Request) code yet, the first part of the guide will show you how to generate a CSR code on GlassFish. The second part will focus on the SSL installation, while the third section will reveal interesting facts about GlassFish and its history. Finally, in the last segment, you’ll discover where to buy the best SSL Certificate for your GlassFish server.

[Generate a CSR code for GlassFish](https://www.ssldragon.com/blog/how-to-install-an-ssl-certificate-on-glassfish/#glassfish-csr)  
[Install an SSL Certificate on GlassFish](https://www.ssldragon.com/blog/how-to-install-an-ssl-certificate-on-glassfish/#glassfish-install)  
[Test your SSL installation](https://www.ssldragon.com/blog/how-to-install-an-ssl-certificate-on-glassfish/#glassfish-test)  
[GlassFish history and versions](https://www.ssldragon.com/blog/how-to-install-an-ssl-certificate-on-glassfish/#glassfish-history)  
[Where to buy an SSL Certificate for GlassFish?](https://www.ssldragon.com/blog/how-to-install-an-ssl-certificate-on-glassfish/#glassfish-where-to-buy)

Generate a CSR code for GlassFish

The first major step you have to perform when dealing with an SSL Certificate is to create a CSR code and send it to the Certificate Authority (your SSL provider). The CSR is a block of text containing details about your website and company. The CAs use it to verify your website’s or/and company’s identity. If your CSR includes erroneous or obsolete information, the CA will not sign your certificate.

You can generate your CSR code in many ways, but the most optimal method for GlassFish is via the **keytool** command line utility. Since GlassFish stores certificates and private keys in special .jks files also called keystores, your first step is to create a new keystore.

1. Type the command below to create a new keystore with a private key  
   keytool -genkey -alias **myalias** -keyalg RSA -keysize 2048 -keystore **mykeystore**.jks  
   We recommend replacing the bold parts with an alias and file name of your choice.
2. Now, the program will ask you to create a password (at least six characters) for this keystore

***Note****:**The keystore and private key passwords must be the same as your GlassFish master password. If you don’t remember your master password and haven’t changed it from the beginning, then the default password should be****changeit.****You can set a new password via the****change-master-password****subcommand of the****asadmin****utility.*

1. Next, the keytool will prompt you to submit your contact details. Follow the examples below to fill in the corresponding fields:
   * **What is your first and last name?** Here, instead of specifying your first and last name, you must include the fully qualified domain name (FQDN) of the site you want to secure. For instance, if you want to install a single or multi-domain certificate, you should enter *com* or *blog.yoursite.com* for a subdomain

***Note****: If you have a Wildcard certificate, add an asterisk in front the domain name (e.g., \*.yoursite.com).*

* + **What is the name of your organizational unit?**You can indicate **IT** or **Web Administration**. For a Domain Validation SSL Certificate, put **NA** NA stands for not available
  + **What is the name of your organization?** If you have a BV or EV SSL Certificate, enter the full name of your officially registered company (e.g., Your Company LLC). For a DV certificate, type NA instead
  + **What is the name of your City or Locality?** Here, specify the city or town where your business is located (e.g., Miami)
  + **What is the name of your State or Province?**Again, enter the name of the region where your company is registered (e.g., Florida)
  + **What is the two-letter country code for this unit?**Provide the two-letter code of your company’s country of origin. (e.g., US). You can find all the country codes [here](https://countrycode.org/)

1. Make sure the info you’ve provided is correct and up to date then press **“y”**
2. The keytool will ask you to set a key password to secure your certificate’s private key. Press enter to make the password identical to the keystore password
3. Now that you have created a keystore file with the private key inside, you can generate your CSR with the following keytool command: keytool -certreq -alias **myalias** -file **domain.csr** -keystore **mykeystore.jks**
4. The **myalias** and **mykestore.jks**attributes should be the same as in the first command. As for **domain.csr**, you should replace it with a custom file name (e.g., yoursite.csr). The domain.csr file will be in the same directory with your keystore

***Note****: Your keystore file is located in the directory where you run the command.*

1. You can open your CSR file with any text editor of your choice (e.g., Notepad). Before sending it to your CA, we recommend one final check for potential typos or errors. Use our [decoder tool](https://www.ssldragon.com/csr-decoder/) to inspect your CSR.

Depending on the validation type of your cert, you’ll have to wait between a few minutes up to a couple of business days for your SSL Certificate files to arrive in your inbox. Once you’ve received them, you can continue with the SSL installation.

Install an SSL Certificate on GlassFish

Before the installation, prepare your SSL Certificate files. Your CA sent them to the email address that you’ve provided. Usually, the files are in an archived folder.

You will have to import the certificate files in the GlassFish keystore that contains your private key. It’s the same keystore that you’ve used to generate your CSR.

1. Your first step is to extract all the files from the .zip folder you’ve received from your SSL provider. It should contain your SSL certificate files in **PEM** (.crt and .ca-bundle) and **PKCS#7** (.p7b and .cer files) formats
2. Next, you need to upload the SSL files to your GlassFish server in one of the formats mentioned in the first step. The **PEM** format requires two commands to import the files, while the **PKCS7#7** just one. Select one of the formats and perform the upload:
   * **PEM (.crt, .ca-bundle)**If you choose the PEM format, you’ll need to upload the CA Bundle files first, and then your primary SSL Certificate file. Enter the following command to import the CA Bundle:  
     keytool -import -trustcacerts -**alias** ca -file file.ca-bundle -keystore mykeystore.jks  
     You can use any name for the alias, as long as it’s different from the keystore’s alias. After the CA Bundle, you can import the SSL Certificate itself. Use the command below to upload it to your server:  
     keytool -import -trustcacerts -**alias** myalias -file file.crt -keystore mykeystore.jks  
     Here, the alias name must match the keystore alias.
   * **PKCS#7 (.p7b, .cer)**If you pick the PKCS#7 format, use the following command to upload all the files at once:  
     keytool -import -trustcacerts -alias **myalias** -file file.p7b -keystore mykeystore.jks  
     The command will ask for your keystore password.  
     The **myalias** attribute should be identical to the one set for your keystore. If you don’t remember your alias, you can see it *via keytool -list -v -keystore mykeystore.jks*command
3. Once your keystore is ready, you should import into the default GlassFish keystore. You can locate it here: *glassfish4/glassfish/domains/****domain1****/config/keystore.jks*

***Note****: GlassFish creates****domain1****by default. If you’ve added a new domain to GlassFish, use its directory instead of the default one.*

1. Here’s the command to import your keystore into the GlassFish one:  
   keytool -importkeystore -srckeystore mykeystore.jks -destkeystore keystore.jks
2. You’ll have to enter the password for both keystores. As we’ve already discussed in the CSR generation section, the password for the GlassFish keystores must be the same as the GlassFish master password for the domain. If the GlassFish, keystore and private key passwords don’t match, your SSL Certificate won’t work
3. After a successful import, you need to update your GlassFish configuration to enable the new SSL certificate. Again, you have two options here. You can perform this action straight from your browser via the GlassFish Administration Console, or manually by editing the domain.xml file.

**GlassFish Administration Console**

If you decide to take the Admin Console route, first you need to enable the secure administration feature for your domain. Run the following command to do it:

asadmin enable-secure-admin **yoursite.com**

Don’t forget to replace**yoursite.com** with your actual domain name.

Once enabled, you can connect to the GlassFish Administration Console via **https://yoursite.com:4848.**

Ignore the self-signed SSL certificate warning and continue browsing the console. Go to **Configurations > server-config > HTTP Service > HTTP Listeners > http-listener-2:**

Click on the “SSL” tab and in the Certificate Nickname field, enter your certificate alias. It is the same as your keystore alias.

Switch back to the “General” tab and change the HTTPS Port to the usual 443. GlassFish uses the 8181 port by default.

Sometimes not all configuration references will update to the new alias in the Administration Console. If this happens to you, don’t worry, you can update them manually in the domain.xml file.

**Domain.xml**

Domain.xml is an alternative way to configure your SSL Certificate in GlassFish. The domain.xml file resides in *glassfish4/glassfish/domains/domain1/config/domain.xml.*

To perform a safe update, we recommend stopping the GlassFish service for your domain, and only afterwards opening the Domain.xml file. To stop GlassFish run the following command: *asadmin stop-domain yoursite.com*. Replace *yoursite.com* with your domain name.

Now you can open the domain.xml file with your favorite text editor. Use the **Ctrl+F** search function to locate the **slas** attribute, the default SSL certificate alias on GlassFish. Next, replace **slas**with your certificate alias. In this article we’ve been using **myalias** as our certificate alias.

If you update all the aliases to your alias, you’ll also install the SSL Certificate for the GlassFish Administration Console.

Save your domain.xml file, and runt the *asadmin start-domain yoursite.com* command to start your domain. Congratulations, you’ve successfully installed your SSL Certificate on the GlassFish server.

Test your SSL installation

After you install an SSL certificate on GlassFish, you can use one of these excellent [SSL tools](https://www.ssldragon.com/blog/the-ultimate-ssl-tools-for-buying-and-testing-an-ssl-certificate/) to check the status of your installation. The instant scans will reveal any potential errors and vulnerabilities that may affect your certificate performance.

GlassFish history and versions

GlassFish is an open-source application server project created by Sun Microsystems and now sponsored by Oracle Corporation. Written for Java EE platform, GlassFish was first released on 6 June 2005. GlassFish allows developers to create portable and scalable applications. It supports Enterprise JavaBeans, JPA, JavaServer Faces, JMS, RMI, JavaServer Pages, servlets, etc.

Below you’ll find all the major GlassFish releases.

* GlassFish 1.0 (a.k.a. Sun Java System Application Server 9.0), released on 4 May 2006
* GlassFish 2.0 (a.k.a. Sun Java System Application Server 9.1), released on 17 September 2007
* GlassFish 3.0 (a.k.a. Sun GlassFish Enterprise Server 3.0), released on 10 December 2009
* GlassFish 3.1 released by Oracle Corporation on 28 February 2011
* GlassFish 4.0 released on 12 June 2013
* GlassFish 5.0 released on 21 September 2017.

Where to buy an SSL Certificate for GlassFish?

The best place to shop for an SSL Certificate for GlassFish is SSL Dragon. We offer incredibly low prices and regular discounts on the full range of our SSL products. We’ve partnered with the best SSL brands on the market to bring your website state of the art encryption. All our SSL certificates are compatible with GlassFish. Here are the types of SSL certificates we sell:

* [Domain Validation](https://www.ssldragon.com/domain-validation-ssl-certificate/)
* [Business Validation](https://www.ssldragon.com/business-validation-ssl-certificate/)
* [Extended Validation](https://www.ssldragon.com/extended-validation-ssl-certificate/)
* [Wildcard](https://www.ssldragon.com/wildcard-ssl-certificate/)
* [Multi-Domain](https://www.ssldragon.com/multi-domain-ssl-certificate/)
* [Code Signing](https://www.ssldragon.com/code-signing-ssl-certificate/)
* [IP Address](https://www.ssldragon.com/ip-address-ssl-certificate/)
* [Email/Documents](https://www.ssldragon.com/doc-email-ssl-certificate/)

To help you pick the ideal SSL certificate for your site, we built two exclusive SSL tools. Our [SSL Wizard](https://www.ssldragon.com/ssl-certificates/ssl-wizard/) needs just a few seconds to find the best SSL deal for your project and budget, while the [Advanced Certificate Filter](https://www.ssldragon.com/ssl-certificates) lets you sort and compare various SSL certificates by price, validation, and features.

If you find any inaccuracies, or you have details to add to these SSL installation instructions, please feel free to send us your feedback at [info@ssldragon.com](mailto:info@ssldragon.com). Your input would be greatly appreciated! Thank you.