Last edited: 10/5/22

Generate Certificate Signing Request

Using the Digicert Certificate Utility, select SSL --> Create CSR

Enter the domain name and any domain alias into the Common Name and Subject Alternative Name Fields.

Create a Service Desk Ticket and attach the CSR to the ticket. Infrastructure will send it to a signing authority and provide the CRTs (Certificate File and CA Bundle File).

Using the Digicert Certificate Utility, verify the CRT and private keys match. Add the CRTs and Key files to the SSL folder in this Teams library.

Getting the key file:

To export the key in IIS (.pfx) or Apache format (.key), go to SSL-->import

Then select the .ca file and add a password

Then export the private key

PFX Certificate Export | Certificate Utility | DigiCert.com

Add Certificates for New Websites

For brand new websites without an existing SSL certificates

Preparing the Files

Rename the CRT and Key files using the following convention:

Key file: example_caloes_ca_gov.key

Certificate file: example_caloes_ca_gov.crt

CA Bundle: example_caloes_ca_gov-ca.crt

If this is a ca.gov site, remove "caloes" from these filenames.

Adding the Files

Upload all three files to /opt/bitnami/apache2/conf and run the following commands:

sudo chown root:root /opt/bitnami/apache2/conf/server*

sudo chmod 600 /opt/bitnami/apache2/conf/server*

where server* is the name of the certificate

Adding a new Virtual Host Entry

Open the bitnami configuration file: /opt/bitnami/apache2/conf/bitnami/bitnami.conf and Add a new VH Entry:

```
<VirtualHost *:443>
   SSLEngine on
   DocumentRoot "/opt/bitnami/apps/wordpress/htdocs"
   ServerName example.caloes.ca.gov
   ServerAlias www.example.caloes.ca.gov
   SSLCertificateFile "/opt/bitnami/apache2/conf/example_caloes_ca_gov.crt"
   SSLCertificateKeyFile "/opt/bitnami/apache2/conf/example_caloes_ca_gov.key"
   SSLCACertificateFile “/opt/bitnami/apache2/conf/example_caloes_ca_gov-ca.crt”

   #Redirect for WWW domain alias only.  Don't add if not using www.
   RewriteEngine On
   RewriteCond %{ HTTP_HOST} ^www\.(.*)$ [NC]
   RewriteRule ^(.*)$ https://%1$1 [R=permanent,L]
</VIrtualHost>
```

The ServerName must match the domain name for the new site.

The Server Alias must match the SANs entered when generating the CSR

Replace the SSLCertficateFile with the path to the new .crt file

Replace the SSLCertificateKeyFile with the path to the new .key file

Ensure you have added the SSLACertificateFile line, and replace with new path

Restart Apache to make the web server pick up the new cert:

Run: sudo /opt/bitnami/ctlscript.sh restart apache

Using the browser, verify the new cert is active and the domain name and domain aliases are correctly configured. Close out the ticket in Service Desk.

Replace Certificates for Existing Websites

For existing websites with SSL certificates already active on the site

Preparing the Files

Create a folder for the new CRT and Key files using the website name and year (Example.caloes.ca.gov 2021)

Add the new files and rename them to match the existing certification files for that site.

FTP into the webserver and download copies of the existing cert files.

Using SSH, rename the existing cert files by adding a -old suffix:

example_caloes_ca_gov-old.crt

Adding the Files

Upload the new cert files and assign them the following ownership and permissions:

sudo chown root:root /opt/bitnami/apache2/conf/server*

sudo chmod 600 /opt/bitnami/apache2/conf/server*

where server* is the name of the certificate

Updating the Virtual Host Entry

The Virtual Host file does not need to be updated if the new certs have the same name as the old ones, unless new alias are being added. In that case, update the ServerAlias field and add rewrite rules as shown in the 'Adding New Certificates' section above.

Restart Apache to make the web server pick up the replaced cert:

Run: sudo /opt/bitnami/ctlscript.sh restart apache

Using the browser, verify the new cert is active and the domain name and domain aliases are correctly configured. After 7 days, remove the -old certificate files from the server.

Bitnami Reference Documentation

https://docs.bitnami.com/azure/apps/wordpress-multisite/administration/create-ssl-certificate-apache/

https://docs.bitnami.com/azure/apps/wordpress-multisite/administration/enable-https-ssl-apache/

https://docs.bitnami.com/azure/apps/wordpress-multisite/administration/force-https-apache/

https://docs.bitnami.com/azure/apps/wordpress-multisite/administration/enable-http2-apache/