

Transcript: SSL Certificate Request and Setup, Base 5.0 and Later

Introduction

When securing your Bomgar sites, applying an SSL certificate signed by a trusted certificate authority assures your customers that your site is secure. Manage your certificates from the Security page of the /appliance interface.

Certificate Request

Start by clicking the **Create** button in the Certificate Installation section. Enter a **Certificate Friendly Name** to identify your certificate request. Select **New Key**, then choose one of the RSA or ECDSA options. You will need to verify with your certificate authority which key strengths they support.

Finally, enter one or more subject alternative names (SAN), such as **support.example.com**, or ***.example.com**.

A SAN lets you protect multiple hostnames with a single SSL certificate. These can be in the form of DNS addresses or IP addresses. A DNS address can be a fully qualified domain name, such as support.example.com, or it can be a wildcard domain name, such as *.example.com.

A wildcard domain name covers multiple subdomains, such as support.example.com, remote.example.com, and so forth. Be sure to define at least one SAN that matches your Bomgar support site name. If you are going to be using multiple hostnames for your site, be sure to define each of those hostnames as additional SANs.

Once you have finished with your configuration, click **Create Certificate Request**. This will create a request in the Certificate Requests section.

Request Submission

You will now need to contact your certificate authority for directions on how to submit your request.

In most cases, requests are submitted by filling out a form on the CA's web site. Some CAs require you to specify the type of server the certificate is for. If this is a required field, you may submit that the server is Apache-compatible.

When prompted to enter the request information, go to the Certificate Requests section on your Bomgar Appliance's Certificates page. Click the subject of your certificate request. Select and copy the request data, and then paste this information into the text area on the CA's request form.

Signed Certificate Upload

After the CA has signed the certificate, they will send it along with the intermediate certificates file back to you. While the Bomgar Appliance supports multiple formats, PKCS #7 files are recommended. Download your certificate to a secure location. This should be a location that can be reached by your Bomgar Appliance.

Go to the **Security** page of your /appliance interface and click the **Import** button. Note that you can view a list of all supported certificate and key file formats here. Upload your signed certificates file to your Bomgar Appliance. Then upload the intermediate certificates chain. Your signed certificate should now appear in the Certificates table.