# BOMGAR™

# Transcript: SSL Certificate Request and Setup Prior to Base 3.3.2

## 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 going to the **Certificate Requests** subsection and clicking the **New Request** button. Enter a **Certificate Friendly Name** to identify your certificate request. Select **New Key**, with a size of either 2048 bits or 4096 bits. You will need to verify with your certificate authority which key strengths they support.

Enter your two-character country code. Your country code can be found by going to iso.org. Enter your state or province if applicable and then your city or locality. Supply your organization name and organizational unit. For your common name, enter your site's fully qualified domain name.

Finally, enter one or more subject alternative names (SAN). A SAN lets you protect multiple host names with a single SSL certificate. These can be in the form of DNS addresses or IP addresses. A DNS address could be a fully qualified domain name, such as support.example.com, or it could 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 at least define one SAN that matches your Bomgar support site name. If you are going to be using multiple host names for your site be sure to define each of those host names as additional SANs.

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

## 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 your Bomgar Appliance's **Certificate Requests** page and click the **Details** link for 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 all formats listed on your appliance's **Import** page, PKCS #7 files are recommended. Download your certificate files 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 then select the **Import** subsection. Upload your signed certificates file to your Bomgar Appliance. Your signed certificate should now appear on the **Certificates** page.

## Server Configuration

To apply your signed certificate to one or more IP addresses, go to the **Server Configurations** subsection and click the **New Advanced Configuration** button.

First, enter a name which will help you identify your configuration later. Choose **Existing Certificate** and then select your signed certificate from the drop-down. Under **Chain**, select **Manually Specified** and then browse to your intermediate certificates file. Check one or more IP addresses to which this certificate should apply. Then click **Continue**.

Your new configuration will appear in the **Server Configurations** list, your signed certificate replacing the SSL certificate for the IP addresses you selected. Note that the default configuration cannot be edited or removed.