Transcript: SSL Certificate Request and Setup, Base 3.3.2 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**, 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 define at least 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 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.

Assign IP

It is important to remember that your new certificate will not secure any hostnames until you assign it to one or more IP addresses. To apply your certificate to an IP address, click the certificate name. At the bottom of the page, select the IP addresses to which this certificate should apply. Then click **Save Configuration**.

This certificate will now serve as the SSL certificate for the IP addresses you selected. Note that the default certificate cannot be edited or removed.