Uploading New SSL Certificates using BMC

The BMC web application is available via TLS-secured (https) access either directly through port 443 or indirectly through port 80 to 443. ACL rules are not applicable to prevent unsecured (http) access. A sample X.509 certificate which is a copy of the BMC, and EMA certificates are shipped along with the SBC shipment. The size of this certificate is 2,048 bits.

The BMC uses the common local certificate store of the SBC (used also for SIP/TLS) rather than having its own separate certificate store. Certificate with RSA keys up to 4,096 bits are supported. However, Sonus recommends using 2,048 bit certificates.

Enter the following URL in the browser to access the SBC BMC GUI:

```
https://<BMC_IP_Address>
```

where BMC IP address is the IP address of the BMC GUI.

The BMC also provides the interface which uploads the self-signed certificate to replace the sample X.509 certificates.

> The SBC is delivered with sample self-signed X-509 certificates. Please be aware that even though these sample certificates will allow you to use HTTPS to access the SBC from the BMC or EMA interfaces, using this protocol with the sample certificates is not a truly secure access method. If your organization requires a more secure access, refer to Generating PKI Certificates.

> **Note**
> The SBC supports a maximum of 4,096 TLS certificates/CAs (both local and remote).

Use the following procedure to upload self signed certificates using BMC:

1. Login to the SBC BMC using the IP address configured in the previous section.

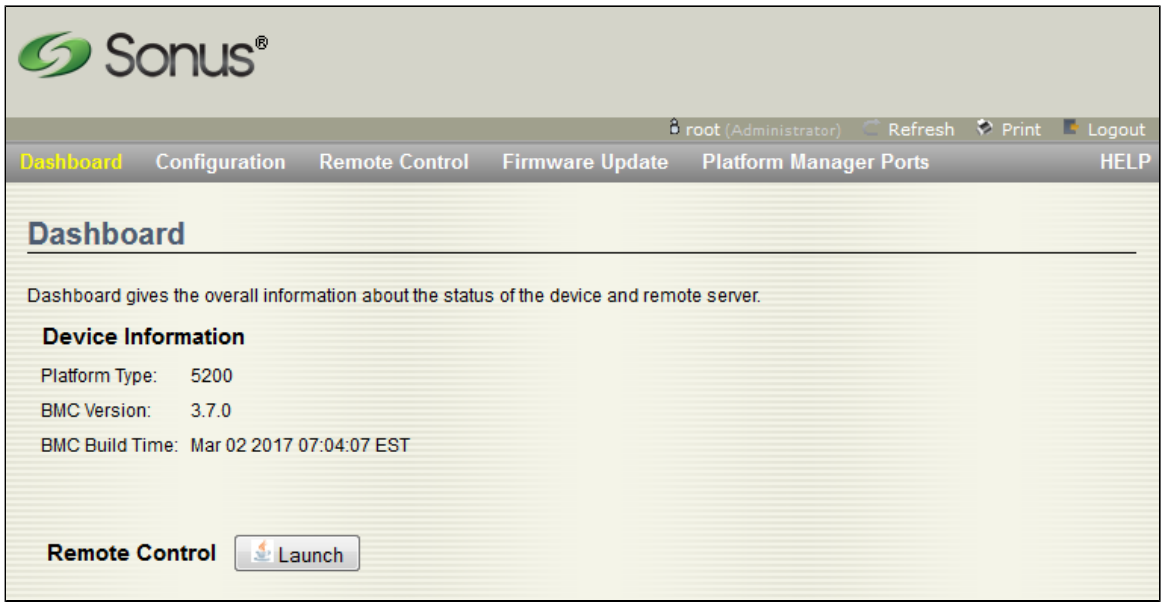
   At the prompt, enter:

   Username: `root`

   Password: `superuser`

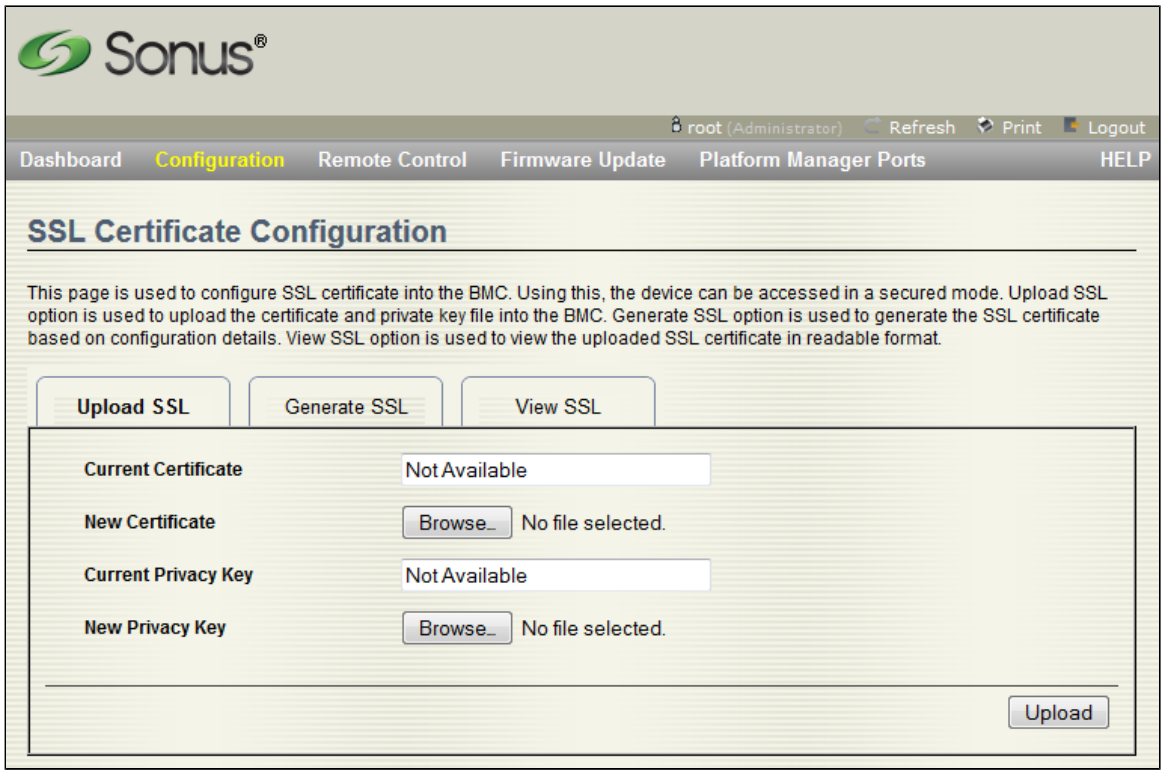
   The SBC BMC main screen appears.

   Figure 1: BMC Main Screen



2. Click **Configuration** > **SSL**. The SSL Certification Configuration screen is displayed.

Figure 2: SSL Upload Screen

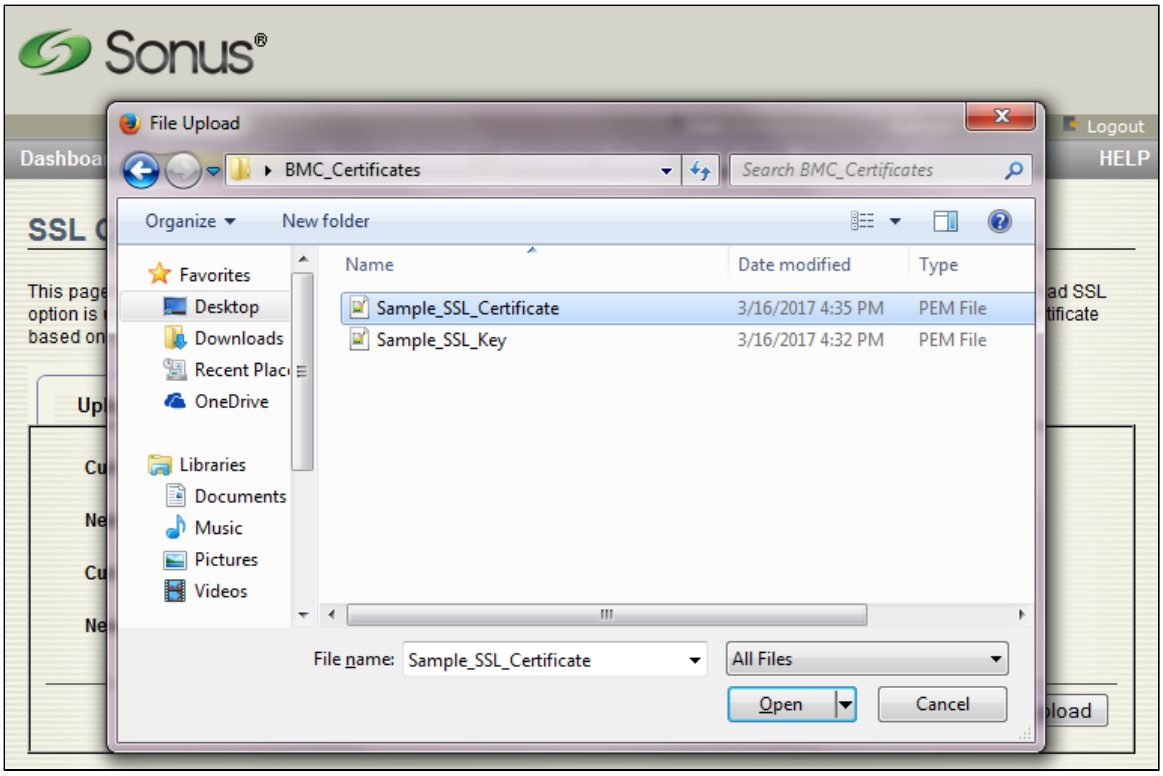


3. Click **Browse** from the Upload SSL tab, and then from the Open dialog, browse to and select the BMC certificate.

> If you require the BMC to send a certificate chain of SSL certificates instead of its own server certificate only, you must import the intermediate CA and/or root CA certificates together with the SBC server certificate in one file. The file must contain all certificates in .pem format.

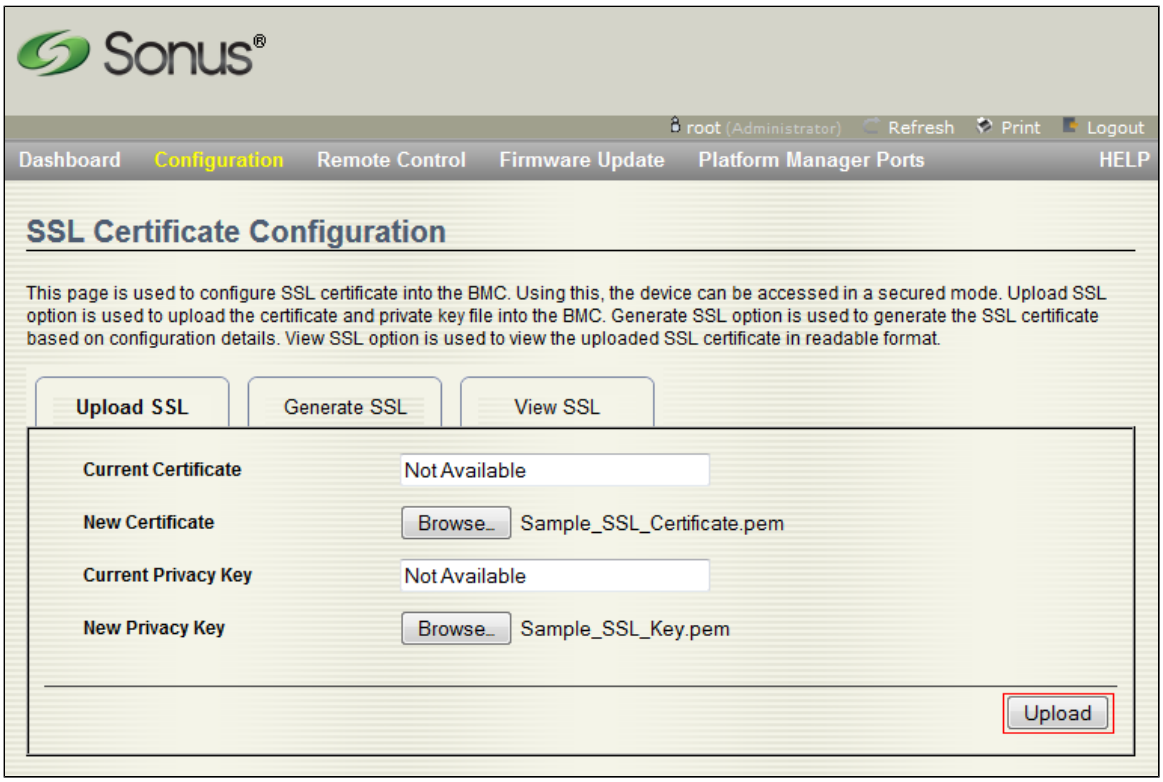
> Perform the same to select the SSL key.

Figure 3: Selecting BMC Certificate



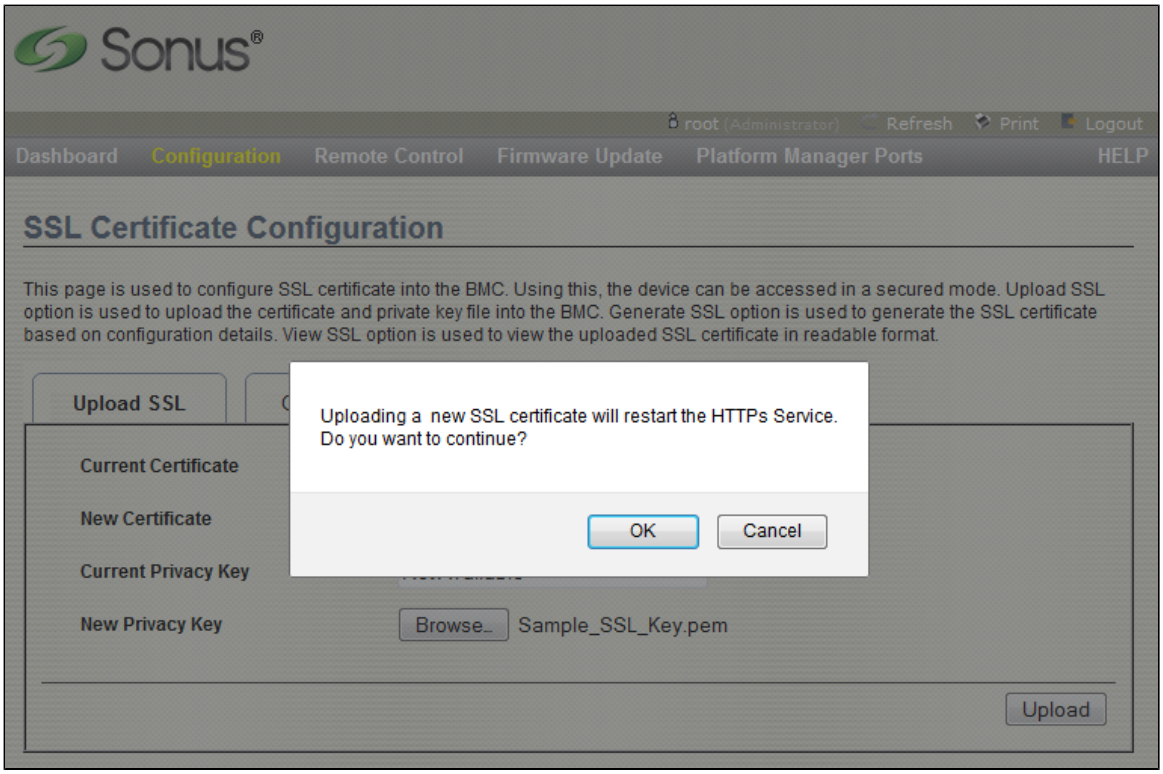
4. Click **Open.** The selected SSL Certificate and the Privacy Key appears in the tab.
5. Click **Upload** to upload the new BMC certificate and the Privacy Key (if any).

Figure 4: Uploading SSL Certificates



6. Follow steps 4 through 6 to upload the Default Privacy Key. A pop up message appears stating that the HTTPs Service need to restart and seeking your permission to proceed.

Figure 5: Successful Upload Message



7. Click **OK** to restart the BMC web server to use the new SSL Certificate.