Tech Note: Using Customer Supplied Certificates on Comrex Opal

Comrex Opal provides for a simple way to allow remote guests to call into a studio with high quality audio feeds. Opal consists of a box that acts as a web server, providing the functionality required to implement the WebRTC protocol for audio.

The WebRTC protocol interworks with web browsers on the guest end. In order to work correctly within a browser, the server (Opal) must provide a standard web security certificate to the browser. This is the same type of certificate (SSL/TLS) used when using any secure web page.

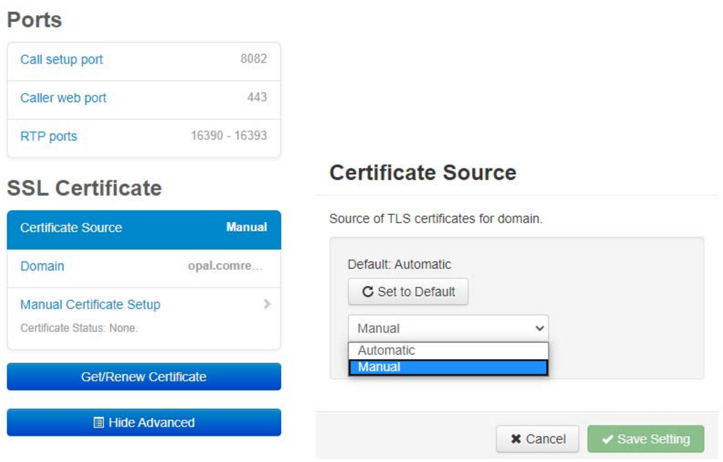
The default way for Opal to obtain these certificates is to use an online resource called **Let's Encrypt**. Opal has a script built-in to obtain this certificate with very little user interaction, and certificates are

In some circumstances, a customer may wish to provide their own certificates for use with Opal. This may be because their domain is controlled and they already have valid certificates for it, or it may be because they have a need to use alternate web server ports.

Using **Let's Encrypt** requires that Opal be able to serve information on TCP port 80 for verification, which is the well-known unencrypted web server port. Some networks block this port, and require that a web server use an alternate port. Also, some customers want to be able to put multiple Opals behind a single IP address, which requires that alternate web server ports be configured. In any event, Opal firmware 1.2p10 and higher allows the generation of CSRs for external certificate generation, as well as the ability to upload certificates, chains, and private keys required to make Opal work. Finally, in the instance where multiple Opals are in use with a single IP address, this firmware has the ability to extract the private key from one Opal for use in others.

Configuring Opal for user-supplied certificates

Figure 1 shows the Toolbox configuration page for the Network settings on Opal. At the bottom of the page is a field to enter the domain name for your Opal (There must be a DNS record of this domain pointing to Opal's IP address). If you select the "**Show Advanced**" option on the bottom of the page, a new field opens that allows you to select between **Automatic** (**Let's Encrypt**) and **Manual** certificate.



Ports

Call setup port 8082

Caller web port 443

RTP ports 16390 - 16393

SSL Certificate

Certificate Source Manual

Domain opal.comre...

Manual Certificate Setup

Certificate Status: None.

Certificate Source

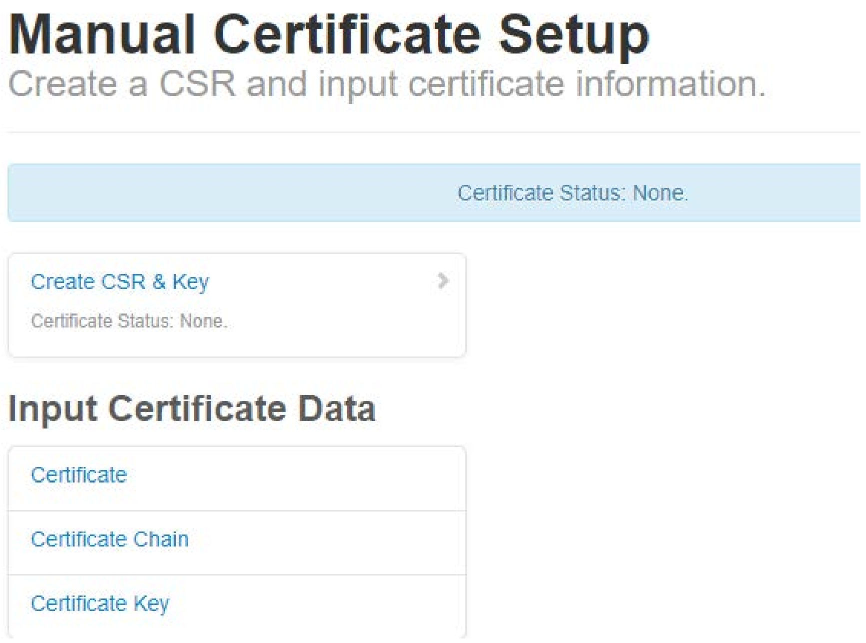
Source of TLS certificates for domain.

Default: Automatic

Manual

Fig. 1

Choose “**Manual**” here and a new option will open labeled “**Manual Certificate Setup**”. Choose this option and you’ll see the menu in Figure 2.



Manual Certificate Setup

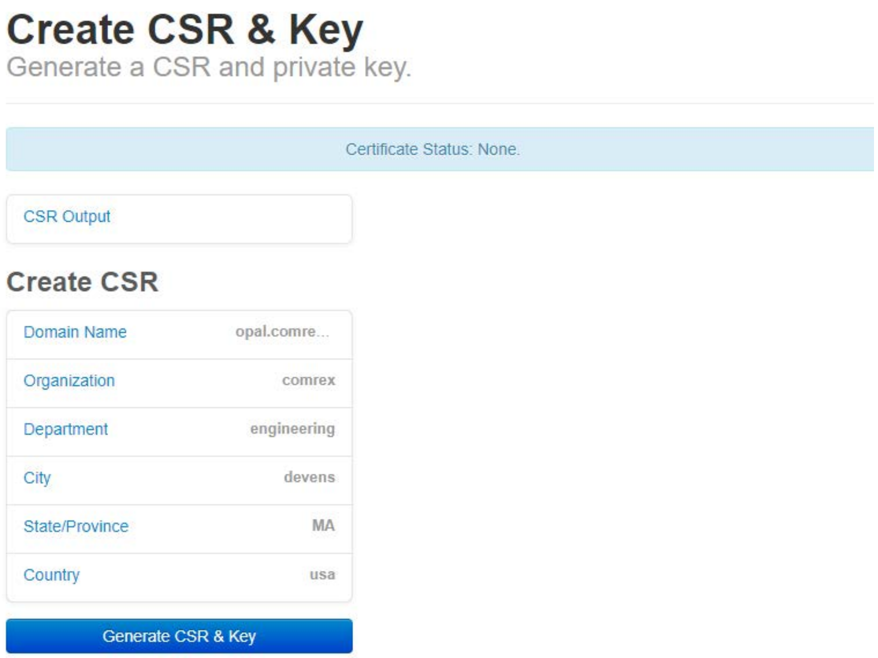
Create a CSR and input certificate information.

Certificate Status: None.

Input Certificate Data

Fig. 2

The first step in manual certificate generation is to generate a Certificate Signing Request. This will be submitted to your Certificate Authority, who will then issue your certificate. Choose “**Create CSR & Key**” from this menu to see the entry fields in Figure 3.



Create CSR & Key

Generate a CSR and private key.

Certificate Status: None.

Create CSR

Domain Name	opal.comre...
Organization	comrex
Department	engineering
City	devens
State/Province	MA
Country	usa

Fig. 3

Complete these fields to the best of your ability. The information will be encoded into the CSR and your certificate. The country field must be the two letter ISO Format country code (e.g US for USA).

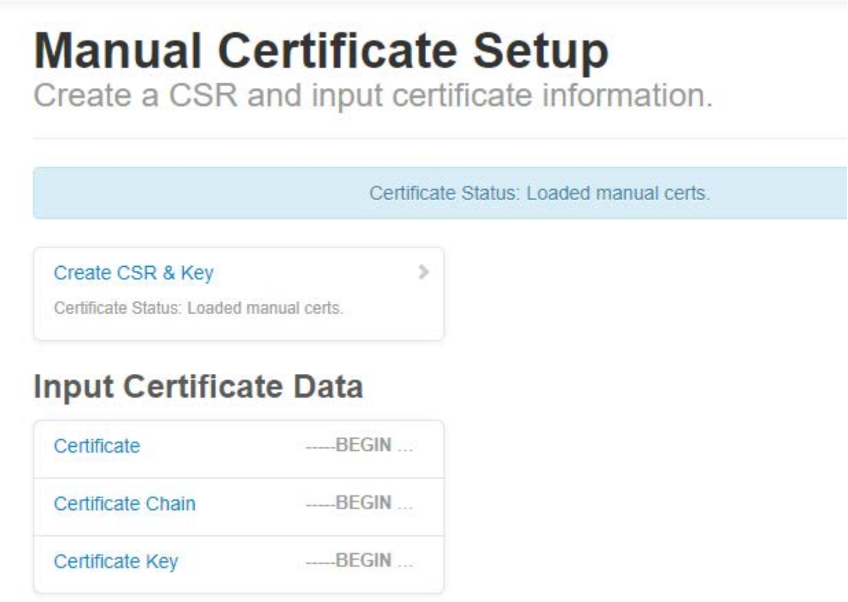
Once the fields are complete, choose "**Generate CSR & Key**". The system will prompt you to wait for one minute, then the "**Restart System**" button will appear. Choose "**Restart System**".

Refresh your browser and re-login. Navigate to **Network** -> **Manual Certificate Setup** -> **Create CSR & Key** -> **CSR output**. Copy all the text from this box. This is your certificate signing request that can be submitted to your CA. You'll typically need to go through an email verification process for your certificate to be issued. Along with the certificate, your CA will issue a second file, known as a chain (or bundle) certificate that looks very much like the certificate file. Both will need to be uploaded to Opal.

Along with your CSR, Opal will generate your "certificate key" for use with the certificate once it is obtained. You don't need to do anything here, as the key is kept in memory and used by default for the next certificate that's uploaded.

Configuring Opal for user-supplied certificates

Figure 4 shows the configuration page under **Network** -> **Manual Certificate Setup** on the Opal Toolbox.



Manual Certificate Setup

Create a CSR and input certificate information.

Certificate Status: Loaded manual certs.

Create CSR & Key

Certificate Status: Loaded manual certs.

Input Certificate Data

Certificate	-----BEGIN ...
Certificate Chain	-----BEGIN ...
Certificate Key	-----BEGIN ...

Fig. 4

Assuming the certificate key was generated by the Opal during the CSR generation process, you will need to upload two text files:

- Certificate

- Chain (or Bundle)

These files may come from your CA labelled with a .txt or .crt suffix, but in each case they are almost always a PEM formatted text file and can be opened with any text editor like Windows Notepad. Once this is done, copy the entire text of the file (including the -----BEGIN----- and -----END---- text) into the appropriate fields on the Opal Toolbox page and select "**Save Setting**".

Once finished, the Opal page will prompt you to select the "**Restart System**" button. Do this, wait 60 seconds, then re-log into Opal. Your certificate status should now show "**loaded manual certs**". As long as the certificate is valid, the DNS record is correct, and the proper ports are forwarded (if behind a NAT router) Opal should be ready to generate invites and take calls.

Duplicating Certificates on Opal

In the scenario where multiple Opals are present behind a single IP address (and on a single domain), only one manual certificate is required. This information will be loaded into each Opal identically.

The certificate and chain/bundle file is the same used for the first Opal. On that first Opal, navigate to **Network** -> **Manual Certificate Setup** -> **Certificate Key** to view the private key that was generated during the CSR generation process. Copy all the text from that field and save it to a .txt file. The contents of that file can now be used for the Certificate Key field in your other Opal(s).

Have questions or need support?

Call us at +1 978 784-1776 or email techies@comrex.com.