Southwest Microwave, Inc.
9055 S. McKemy Street
Tempe, AZ 85284
(480) 783-0201 Fax (480) 783-0401

TECHNICAL NOTE # 1002

Signed Server Certificate Creation with a Custom CA Certificate for POE-S Devices

All Southwest Microwave POE-S technologies have the option of being run in Unencrypted browser mode (Port 80), or SSL-encrypted browser mode (Port 443). On initial setup, Unencrypted mode is default.

While many customers rely on site network security settings to achieve the required security level, some elect to change HTTP(S) port settings from Unencrypted to SSL-Encrypted.

If browser encryption is a requirement for your system, the technical manuals for each Southwest Microwave INTREPID™ POE-S product has clear and detailed instructions on how to achieve this. If you are working through these steps and encounter issues, the likelihood is that your browser has been updated, patched to improve operation or is a different version than shown in our manual.

This Technical Note provides several options for achieving browser encryption:

1. Generate a self-signed certificate.
2. Use a free tool for creating a custom CA and use this CA to sign server certificates.
3. Purchase and download a custom certificate from a commercial Certificate Authority (CA).

Option 1: Generating a Self-Signed Certificate

By using our self-signed certificate generation process we are creating a secure connection. However, recent updates in most major browsers (Chrome, Edge, Firefox) no longer identify self-signed certificates as secure because they are not being generated from a registered Certificate Authority.

An example of this is the way Chrome now treats self-signed certificates. When SSL-Encryption is enabled on the POE-S device, a new link is generated. Once selected, the “Your connection is not private” page is displayed, but the “Advanced” button is no longer shown as an option to proceed. To proceed in accessing our POE-S web page, click in any white space in the browser window and type “thisisunsafe”. Wait at least 30 seconds for this to process, and do not click anything else during this time.

Once these steps are completed, the data is encrypted and secure, but the browser display does not reference that it is. Instead, the web browser displays this “Not secure” icon with https crossed out in the URL bar as shown in Figure 1.

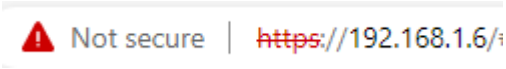

Figure 1

If this scenario is not acceptible for your site, proceed to Option 2.

Option 2: Use a free tool for creating a custom CA and use this CA to sign server certificates.

One free tool that will enable the creation of a custom CA that can be used to sign server certificates is **XCA (X Certificate and Key Management)**. This can be downloaded at:

https://hohnstaedt.de/xca/index.php/download.

Follow the instructions for creating the CA, installing this CA into the Windows Trusted Root Certificate Authorities, then creating and applying the signed server certificate and the private key (*.pem format) into the POE-S devices.

Note that this free tool is not a Southwest Microwave product and should be independently vetted by the IT or Cybersecurity Administrator of any site considering this option. If the free option is not approved, proceed to Option 3.

Option 3: Purchase and download a custom certificate from a commercial Certificate Authority (CA) to replace the auto generated self-signed certificate in our POE-S devices.