SSL Web Certificates

Introduction

The default SSL web certificates in sipXecs are self-signed certificates, meaning there is not a valid certificate authority to verify them against. This results in popular web browsers such as Microsoft Internet Explorer, Google Chrome, Apple Safari, and Mozilla Firefox displaying onerous messages regarding website security when accessing the sipXecs web portal. This guide will step the sipXecs administrator through generating a certificate signing request (CSR) and installing the new web certificates.

Generating a 1024 bit Certificate Signing Request (CSR)

To generate a 1024 bit certificate signing request in sipXecs log in as a user with administrative rights (such as superadmin). Once you have logged in, browse to **System >> Certificates**. You will be presented with the Generate CSR page. Enter the correct information for all fields, then click **Generate**. The 1024 bit certificate signing request will be generated. Submit this certificate signing request to the certificate authority you wish to sign the certificate.

Generating a 2048 bit Certificate Signing Request (CSR)

Most certificate authorities now require 2048 bit or greater certificate signing requests but by default sipXecs generates 1024 bit certificate signing requests. Creation of 2048 bit certificates from sipXconfig is not yet supported. Alternatively, a 2048 bit CSR can be generated from the command line, changing the output filenames to match your certificate name:

```
openssl req -nodes -newkey rsa:2048 -keyout sipx.ezuce.com.key -out sipx.ezuce.com.csr
```

> ⚠ Fill in the requested values with your own information. The most important of these is **Common Name** which will be the hostname of your configuration server. If creating a CSR for a wildcard certificate, you will need to enter ***.domain.tld** where **domain.tld** is the top level domain of your server.

> Wildcard certificates only support one subdomain level. What this means is that if your server name is **server.subdomain.domain.tld** and you register a wildcard certificate only for ***.domain.tld** your certificate will not be recognized by any browser. You would need to purchase a wildcard certificate for ***.subdomain.domain.tld** for the wildcard certificate to be properly recognized.

```
Generating a 2048 bit RSA private key
.....+++
.........................+++
writing new private key to 'sipx.ezuce.com.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:Massachusetts
Locality Name (eg, city) [Default City]:Andover
Organization Name (eg, company) [Default Company Ltd]:eZuce, Inc.
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:sipx.ezuce.com
Email Address []:sipx@ezuce.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Copy the certificate signing request file and the private key from the server using a SFTP/SCP program such as WinSCP. Once copied, you may now submit the resulting CSR to you SSL provider. Be sure to back up your key to a safe place.

Preparing For SSL Certificate Installation: CA Chaining Certificates

Most certificate authorities now implement CA chaining as a method of verifying smaller certificate signing authorities against larger, more well-known signing authorities. These chaining certificates must be installed alongside the SSL certificate issued by the certificate signing authority. sipXecs now allows direct uploading of chaining certificates under **System >> Certificates >> Import Web Certificate.**

Installing SSL Web Certificate

log into the sipXecs web portal as a user with administrative rights (such as superadmin). Once you have logged in, browse to **System >> Certificates**. Choose **Import Web Certificate** on the left pane. Click **Choose File** or **Browse** (depending on your browser) and select the **SSL certificate,** the **Key File (mandatory)**, and optionally **Certificate Chain File** and/or **CA Certificate File** to upload. Once you have selected the certificates, click the **Import** button. sipXecs will import the certificates but you should restart Apache manually by invoking the following command:

```
service httpd restart
```

You may have to close and reopen your browser for the SSL certificate to properly validate

Changing the SSL Web certificate will also change the openfire IM server certificate