

Secure Socket Layer (SSL)

supportcenter.nc4.com/hc/en-us/articles/218312257-Secure-Socket-Layer-SSL-

SSL protocol provides cryptographic security and establishes a secure connection between two parties (in E Team's case, between the browser client and the E Team server). The SSL protocol offers these security benefits:

- Data is encrypted to and from clients, so privacy is ensured during transactions.
- An encoded message digest accompanies the data and detects any message tampering.
- The server certificate accompanies data to assure the client that the server identity is authentic.
- The client certificate accompanies data to assure the server that the client identity is authentic. Client authentication is optional and may not be a requirement for every organization.

Use of SSL mandates use of Internet Explorer 6.0 or better. The SSL port must be open on the firewall/network to support use of the SSL protocol, and a secure server ID issued by Certificate Authorization is required. *Also ensure that the HTTPS or the HTTP and HTTPS option is used during the installation.*

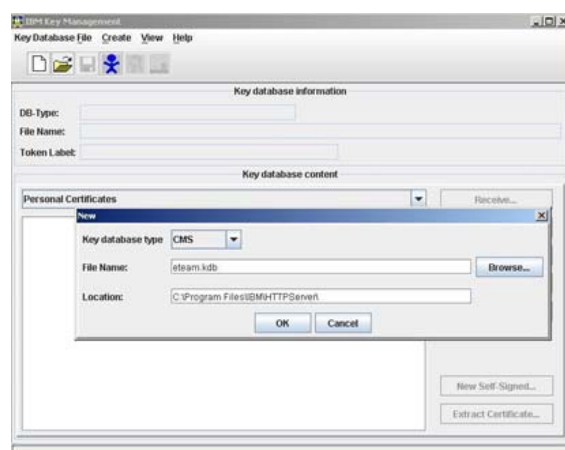
How SSL Works

When SSL is enabled, all communications between the browser client and the server are encrypted the moment that a session is initiated with the E Team application. Encryption includes the username and password.

Generating a Certificate Signing Request

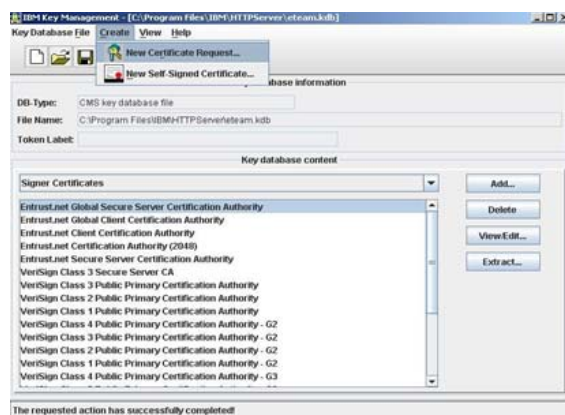
The following steps must be performed to generate a Certificate Signing Request (CSR).

1. Click on Start, Programs, IBM HTTP Server V6.1, then select Start Key Management Utility.
2. Click on Key Database File and select New.
3. Change the Key Database type to CMS.
4. Enter a file name. In this example, we use eteam.kdb for the file name. Note the location of the file being saved is C:\Program Files\IBM\HTTPServer.



5. Click on OK.
6. Enter a password for this Keyring and select Stash the password to a file.
7. Click on OK.





8. Click on *Create* and select *New Certificate Request*.
9. The information on the next screen should be entered carefully and accurately.



- Key Label: Key Label is just a generic name
 - Key Size: Leave the key size at 1024 bits
 - Common Name: The common name is the name you will use to access the E Team application so it must MATCH exactly. You do not need to enter http or https at the beginning, just the Fully Qualified Domain Name (FQDN). If you are not sure what your FQDN is, please contact NC4 support.
 - Organization: Enter your Organization name.
 - Organization Unit (optional): Enter your Organization unit. This field is optional.
 - Locality (optional): Enter your City or County.
 - State/Province (optional): Enter your State or Province. Names must be spelled out in full and not abbreviated.
 - Zipcode (optional): Enter your Zipcode.
 - Country or region: Enter your Country or region.
10. When all fields have been accurately completed, enter the name of the file where the certificate request will be stored. For example, C:\ProgramFiles\IBM\HTTPServer\certreq.am
 11. A confirmation window will be displayed upon successful creation of the CSR file.



Merging the Signed Certificate into the Keyring

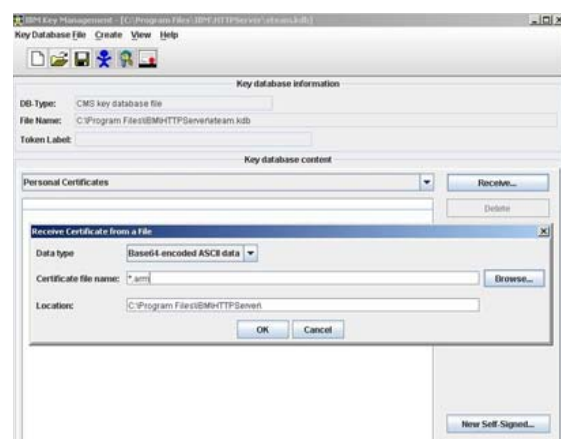
Depending on your CA, the process of digitally signing the certificate could take up to 48 hours. Once you receive the signed certificate from the CA, you will need to merge it to the original key. The following steps are required to complete this task:

1. Save the file you received from your CA onto the server. Preferably, use cer as the extension.
2. Click on Start, Programs, IBM HTTP Server V6.1, Start Key Management Utility.
3. Click on Key Database File and select Open.
4. Point to the original key file you created. In the example in Step 1, it was etteam.kdb.

5. Enter the password when prompted.
6. Click OK
7. On the main screen, click on the drop down menu under Key Database Content and select Personal Certificate.

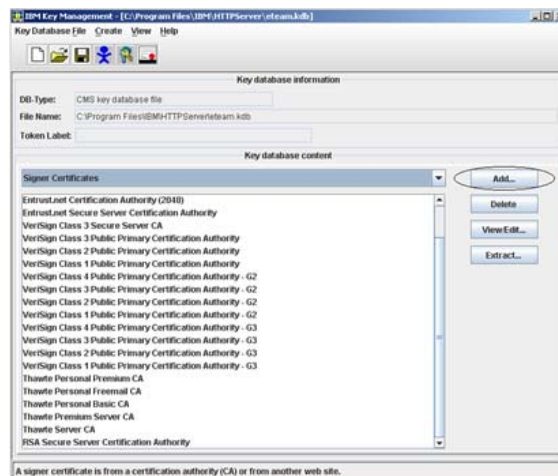


8. Click on Receive and point to the file you received from the CA.
9. Click OK



10. The Keyring file is now signed and ready for use.

If you get an error message stating that the Signer's certificate does not exist in the Keyring, it is because the root and intermediate certificate of the CA is not included in the Key file database. By default, the only signer certificates installed are from Entrust, Verisign, Thawte, and RSA Secure Server Certification Authority. In this case, you will need to download your CA's intermediate and root certificates from their Website and Add them to the Signer Certificates.



Your SSL key is now ready to be copied to the IBM HTTP server. You need to copy the following two files from C:\Program Files\IBM\HTTPServer into the keys folder in the IBM HTTP install directory C:\Program Files\IBM\HTTPServer\Conf\Keys

- The file with extension kdb (example: eteam.kdb)
- The file that contains the stashed password with extension sth (example: eteam.sth)

Make sure the location defined in the httpd.conf file matches the location and file name specified.