SSL Configuration

FileCloud runs on Apache web server.

- Apache server can be configured to serve the website securely using HTTPS protocol.
- To enable the HTTPS protocol, you will need an SSL certificate.

💡 *In the following section, to display more information, click on a question.*

If you are using Active Directory and want to:

- Add AD users
- Change AD passwords
- Secure the connection to Active Directory

Then you will need to configure additional settings and also install an SSL certificate on the AD server.

This topic does not relate to securing connections with your AD Server.

➡ For that information, please read Connecting to AD via SSL

SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.

To be able to create an SSL connection a web server requires an SSL Certificate. When you choose to activate SSL on your web server you will be prompted to complete a number of questions about the identity of your website and your company. Your web server then creates two cryptographic keys - a Private Key and a Public Key.

The complexities of the SSL protocol remain invisible to your customers. Instead their browsers provide them with a key indicator to let them know they are currently protected by an SSL encrypted session - the lock icon in the lower right-hand corner, clicking on the lock icon displays your SSL Certificate and the details about it. All SSL Certificates are issued to either companies or legally accountable individuals.

➡ To learn more about SSL, read knowledge base articles on the SSL web site.

To enhance the security of the Root certificate, two intermediate certificates are created from which SSL certificates are signed and issued.

- An intermediate certificate is a subordinate certificate issued by the trusted root specifically to issue end-entity server certificates.

The result is a certificate chain that begins at the trusted root CA, through the intermediate and ending with the SSL certificate issued to you. Such certificates are called chained root certificates.

Creating certificates directly from the CA root certificate increases the risk of root certificate compromise, and if the CA root certificate is compromised, the entire trust infrastructure built by the SSL provider will fail. The usage of intermediate certificates for issuing SSL certificates to end entities, therefore, provides an added level of security. You must install the intermediate certificate in your Web server along with your issued SSL certificate to complete the trust chain and allow the certificate to be effective.

Once you’ve got your certificate files, seeing your file extension will allow you to know what’s in the file, and if you need to convert them.

File Extension	Contents
*.pem	Concatenated certificate container files Frequently required for certificate installations when multiple certificates are being imported as one file.

*.crt *.cer	The *.crt and *.cer file formats are interchangeable and contain the same information. the *.crt file is a Microsoft convention and can be easily converted to *.cer. An SSL certificate contains both: *.key = the private key to the certificate *.crt = the signed certificate
*.ca-bundle	A file that contains root and intermediate certificates. • The end-entity certificate along with a CA bundle constitutes the certificate chain. The chain is required to improve compatibility of the certificates with web browsers and other kind of clients. This allows browsers to recognize your certificate so that no security warnings appear.
*.pfx	This is an archive file format for storing several cryptographic objects in a single file. • contains the end-entity certificate (issued to your domain) • a matching private key • may optionally include an intermediate certification authority (a.k.a. CA Bundle). All this is wrapped up in a single file which is then protected with a pfx password.

What do you want to do?

➡ Use SSL on Windows

➡ Use SSL on Linux

➡ Convert a PFX to a PEM SSL Certificate