

Using Your Own SSL Certificate

Background

During the installation of MailStore Server, an SSL certificate is generated which all MailStore Server components use when an encrypted connection is to be established. Since the certificate is issued to the server name *MailStoreServer* and does not come from a reliable certification authority (CA), it is not trusted by the client side.

Because of this, the following warning message is displayed when calling up MailStore Web Access via HTTPS (SSL):

One option for resolving this issue is to make the server on which MailStore Server is installed available under the host name *MailStoreServer* (e.g. by adding an A- or CNAME record in the DNS) and installing the certificate in the container of trusted root certification authorities on the clients. Because these installations involve a relatively high administrative overhead, MailStore Server provides the option to use signed certificates of your own company CA or certificates of a public certification provider (e.g. VeriSign, eTrust etc.).

To configure MailStore Server for the use of your own certificate, please proceed as follows:

Creating a Certificate Signing Request

Multiple tools are available to create a certificate signing request (CSR). Please understand that it does not fall under the scope of this article to explain their usage.

The most commonly used tools to manage SSL certificates are:

- Certificates MMC snap-in
- certreq.exe
- openssl.exe

Those programs create a private key first, followed by the certificate signing request. The certificate signing request, but NEVER the private key, must be sent to the certificate authority. After the certificate signing request was signed by the certificate authority, the actual certificate is sent back to you.

Please notice, that the private key that was used to create the certificate signing request must reside in the same certificate store as the certificate. This usually is "Certificates (Local Computer) > Personal > Certificates" for services running under the local system account.

Installing the Certificate

- Log on to the server as administrator.
- Click on *Start / Execute*.
- Execute the command *mmc*.
- Select *File / Add/Remove Snap-In / Add / Certificate*
- Select *Local Computer Account* and then *Local Computer*.
- Click on *Finish* and close any open dialog windows.
- In the management console, select *My Certificates / Certificates*.
- Right-click on the folder *Certificates* and select *All Tasks / Import*
- Follow the instructions in the wizard and select the file containing the certificate and the private key, if applicable.
- On the page *Certificate Store* select the container *My Certificates* and finish the wizard.
- The certificate is now shown in the container *My Certificates*.
- To verify this and to make sure that the private key for the certificate is available, open the certificate with a double-click.

Using the Certificate with MailStore Server

- Open the MailStore Server Service Configuration.
- Select *IP Addresses and Ports*.
- In the section you want to change to certificate for, click on the button next to the *Server Certificate* field and select *Select from Certificate Store...*
- Choose the new certificate from the certificate store.
- Confirm your entries and restart the MailStore Server service.

⊖Revision #1

★Created 30 December 2021 17:02:27 by Mahesha Damayanthi

✎Updated 30 December 2021 17:03:56 by Mahesha Damayanthi