Deploying a Self-signed SSL Certificate

Background

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

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

This article describes the option to deploy self-signed certificates using a group policy. An alternative is to use officially signed SSL certificates issued by your own company CA or a trusted external certificate authority, such as VeriSign or eTrust, which is described in chapter Using Your Own SSL Certificate.

To configure MailStore Server and your clients for using a self-signed certificate, please proceed as described in the following.

Creating a Self-Signed Certificate

The self-signed certificate created during the installation of MailStore Server is issued to the server name *MailStoreServer*.

If the DNS host name of the server does not correspond to *MailStoreServer* and if no corresponding A- or CNAME record exists on the DNS server, first a new self-signed certificate with the appropriate host name must be created. Please proceed as follows:

- Open the MailStore Server Service Configuration.
- Click on *IP Addresses and Ports*.
- Click on the button next to the field *Server Certificate* and select *Create Self-Signed Certificate...*
- As name for the new certificate, enter the server name with which the MailStore server can be reached, e.g. mailstore.mydomain.local, and click on *OK*.
- If necessary, replace all additional server certificates with the new certificate. To do so, click on the button next to the *Server Certificate* field and select *Select from Certificate Store...*

Deploying a Self-Signed Certificate

Before the self-signed certificate can be deployed, it must be exported from the current certificate store. Please proceed as follows:

- Open the MailStore Server Service Configuration.
- Click on *IP-Adressen and Ports*.
- Click on the certificate.
- Open the *Details* tab.
- Click on *Copy to File*.
- Follow the instructions of the certificate export wizard to export the certificate *without* the private key in DER encoded format into a file.

Once the certificate has been exported to a file, create a group policy as described in chapters MailStore Client Deployment or MailStore Outlook Add-in Deployment and to deploy the certificate customize it as follows:

- Open the group policy object using the *Group Policy Management Editor* of your Windows server.
- Expand the *Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies*.
- Right-click on *Trusted Root Certification Authorities* and select *Import...*.
- Follow the instructions of the certificate import wizard to import the certificate from the file.
- Under *Public Key Policies* open the properties of the *Certificate Services Client - Auto-Enrollment*
- Change the *Configuration Model* to *Enabled* and click on *OK*.
- Under *Public Key Policies* open the properties of the *Certificate Path Validation Settings*.
- Place a checkmark next to *Define these policy settings* and click *OK*.

The group policy will be enabled once the workstation is restarted.

Revision #1
Created 30 December 2021 14:28:48 by Mahesha Damayanthi
Updated 30 December 2021 14:29:40 by Mahesha Damayanthi