1. Appendix
   1. Configuring HTTPS between Vision application server and client

This section describes the procedure to configure HTTPS between Vision application server and Vision client machines. Following major steps must be performed for this configuration:

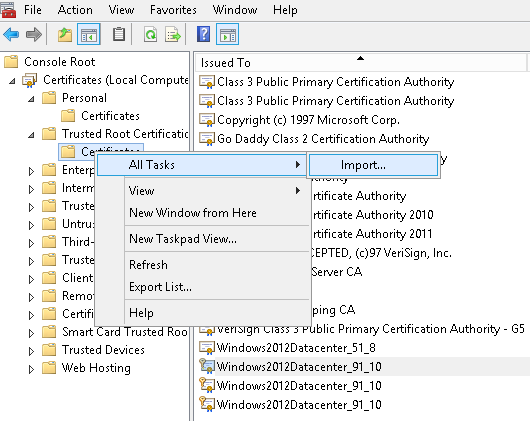
1. Import trusted secured certificate in Windows Certificate store

Details are mentioned in below sections.

* + 1. Import trusted secured certificate in Windows Certificate store

Customers must have secured certificate from any trusted source. During configuration of secured certificate, customers must use TLS v1.1 or higher to ensure minimum required encryption strength. Certificates are \*.pfx or \*.cer files which will be imported into Windows Certificate store.

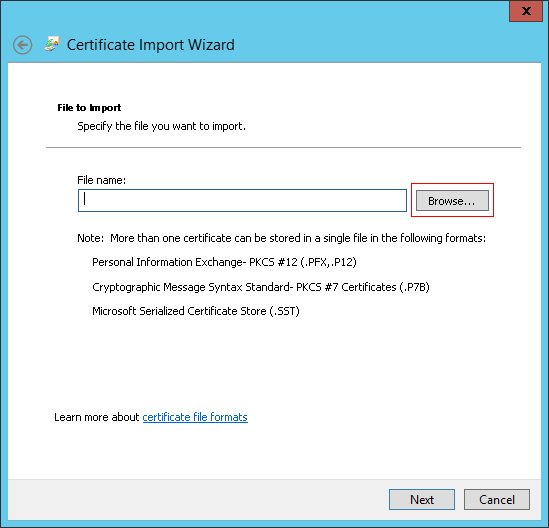
On any version of Windows, open “Certificates” management console and browse to “Trusted Root Certification Authorities”. (One of the option is to click onStart, then open “Run” dialog window and type mmc. This will open “Microsoft Management Console”. Click on File Menu and select Add/Remove Snap In. From the window, select “Certificates”. Add Certificates. Select “Computer Account”. Then follow next to finish. Then Ok). Select “Import” option as depicted below:



Certificate import option

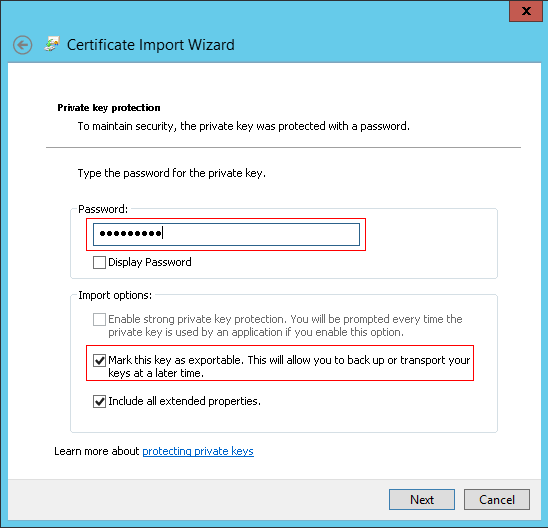
Make sure to select desired “Host Name” / “Issued To” title during certification procurement process. This title shall be used in next step when this certificate is associated with Vision application server directory.

System shall open Import dialog window to select a certificate file (by clicking on “Browse” button as displayed below):



Certificate import wizard with file name selection option

After file selection, next step is depicted in below image:



Certificate import wizard with private key option

Following must be performed in this step:

* Enter password as received from the trusted root certification authority along-with certification file
* Check-mark the option specifying exportable key (This option shall be used to export the key when required)

After import process, new certificate shall be displayed in “Trusted Root Certification Authorities” list. Copy the displayed certificate from this folder and paste it into “Personal” certificates folder.