

# How to install a self-signed Digital Certificate in Attendant Console operator's workstation

## Applies to:

Imagicle UC Suite ver. 2021.Winter.1 and above

For Attendant running on Windows PC Client only

## Description:

Starting from 2021.Winter.1 release, the proprietary TCP connection between Imagicle Attendant Console client and UC Suite server can leverage TLS 1.2 encryption. If a self-signed Digital Certificate is used, then the same Certificate must be installed in both server and client side.

## How-to:

- Please copy your Digital Certificate in pfx format on your PC where Attendant Console client is installed. You can obtain the correct Certificate by exporting it from UC Suite server: IIS Control Panel > Server Certificates > Export.
- Double-click on Certificate to launch the import wizard.

←  Certificate Import Wizard

## Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

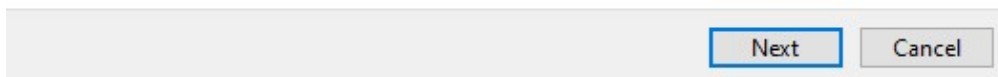
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

Current User

Local Machine

To continue, click Next.



- You can choose to install the Certificate for current user only, or for whole local workstation. Hit Next to continue.

## File to Import

Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX, .P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialised Certificate Store (.SST)

- Certificate path appears. No need to change it. Just hit Next to continue.

## Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

Display Password

Import options:

- Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
- Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
- Protect private key using virtualised-based security(Non-exportable)
- Include all extended properties.

Next

Cancel

- Enter here the password which has been used during Certificate export. Hit Next.

## Certificate Store

Certificate stores are system areas where certificates are kept.

---

Windows can automatically select a certificate store, or you can specify a location for the certificate.

- Automatically select the certificate store based on the type of certificate
- Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

Browse...

Next

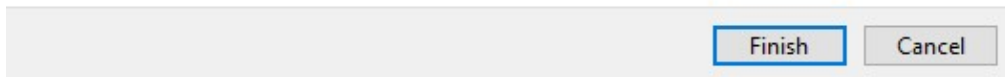
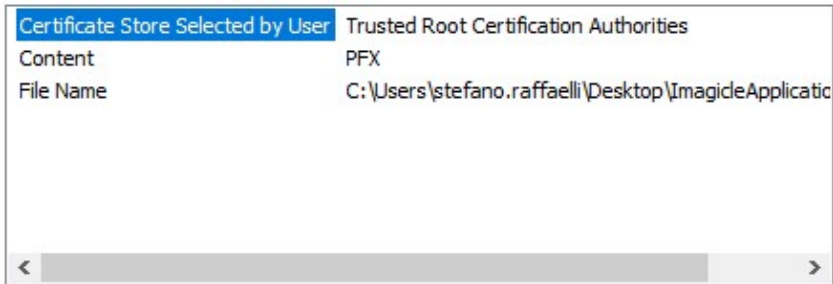
Cancel

- Please choose to save the Certificate into Trusted Store. Hit Next to continue.

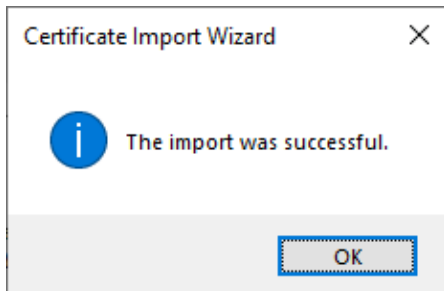
## Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:



- Summary page is displayed. Please hit Finish to complete the import procedure.



- If you get an error message, please check your Digital Certificate with your IT administrator.