

Certificate Import Wizard

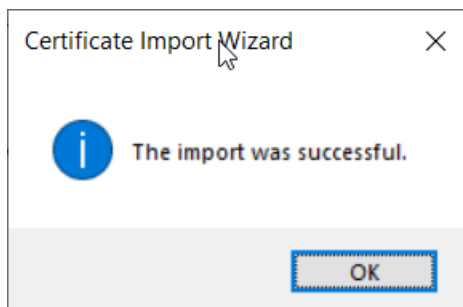
VPN Configuration Steps:

1. Install by running "InstallVPN-Signed.ps1" via right-click "Run with PowerShell"
2. If an Execution Policy change prompt appears, make sure to enter "Y" for Yes and press Enter
3. Your p12 private cert password is your mobile number in reverse converted to hexadecimal uppercase
4. "ThirdSight" VPN shortcut will be created on your desktop and it uses the rasdial.exe command to initiate the VPN connection
5. Next install the 2nd VPN shortcut "Add-3S-VPN.ps1" via right-click "Run with PowerShell"
6. There should now be two separate VPN shortcuts on your desktop, one "ThirdSight" VPN and another "3S VPN"
7. Set the VPN metrics to take priority over your Wifi/LAN interfaces:


<https://thirdsight.net/3s/?xmail-id=263973ab-4e58-44c0-ae5c-e220bf50d095&wkspc-id=522>



Password

33350B31



Welcome



  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.

Next

Cancel

Next



  Certificate Import Wizard

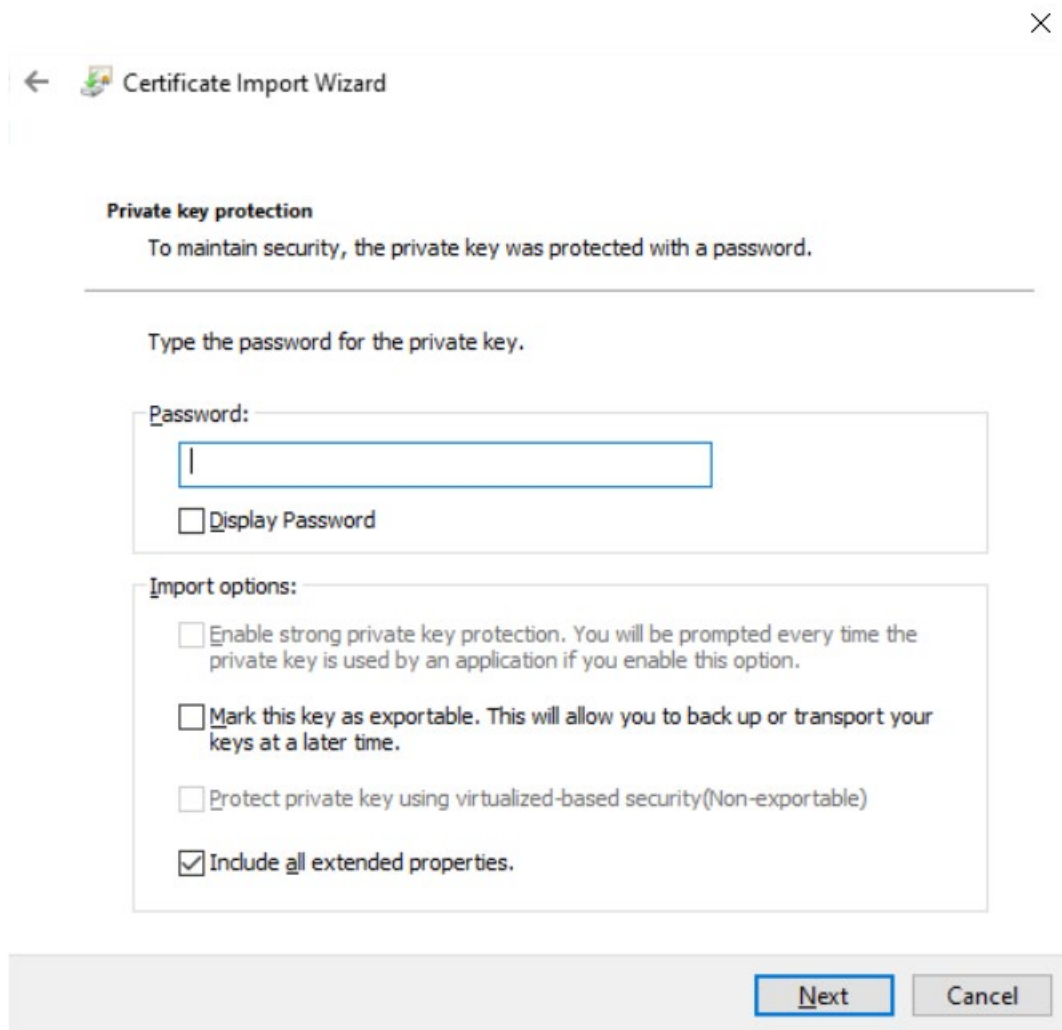
File to Import
Specify the file you want to import.

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 Serialized Certificate Store (.SST)

[Next](#)



The image shows a Windows dialog box titled "Certificate Import Wizard". It has a back arrow icon on the left and a close 'X' icon on the right. The main content area is titled "Private key protection" and contains the text "To maintain security, the private key was protected with a password." Below this is a horizontal line and the instruction "Type the password for the private key." There is a "Password:" label followed by a text input field. Below the input field is a checkbox labeled "Display Password". Further down is a section titled "Import options:" containing four checkboxes: "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 virtualized-based security(Non-exportable)", and "Include all extended properties." The last checkbox is checked. At the bottom right of the dialog are two buttons: "Next" and "Cancel".

← Certificate Import Wizard

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.

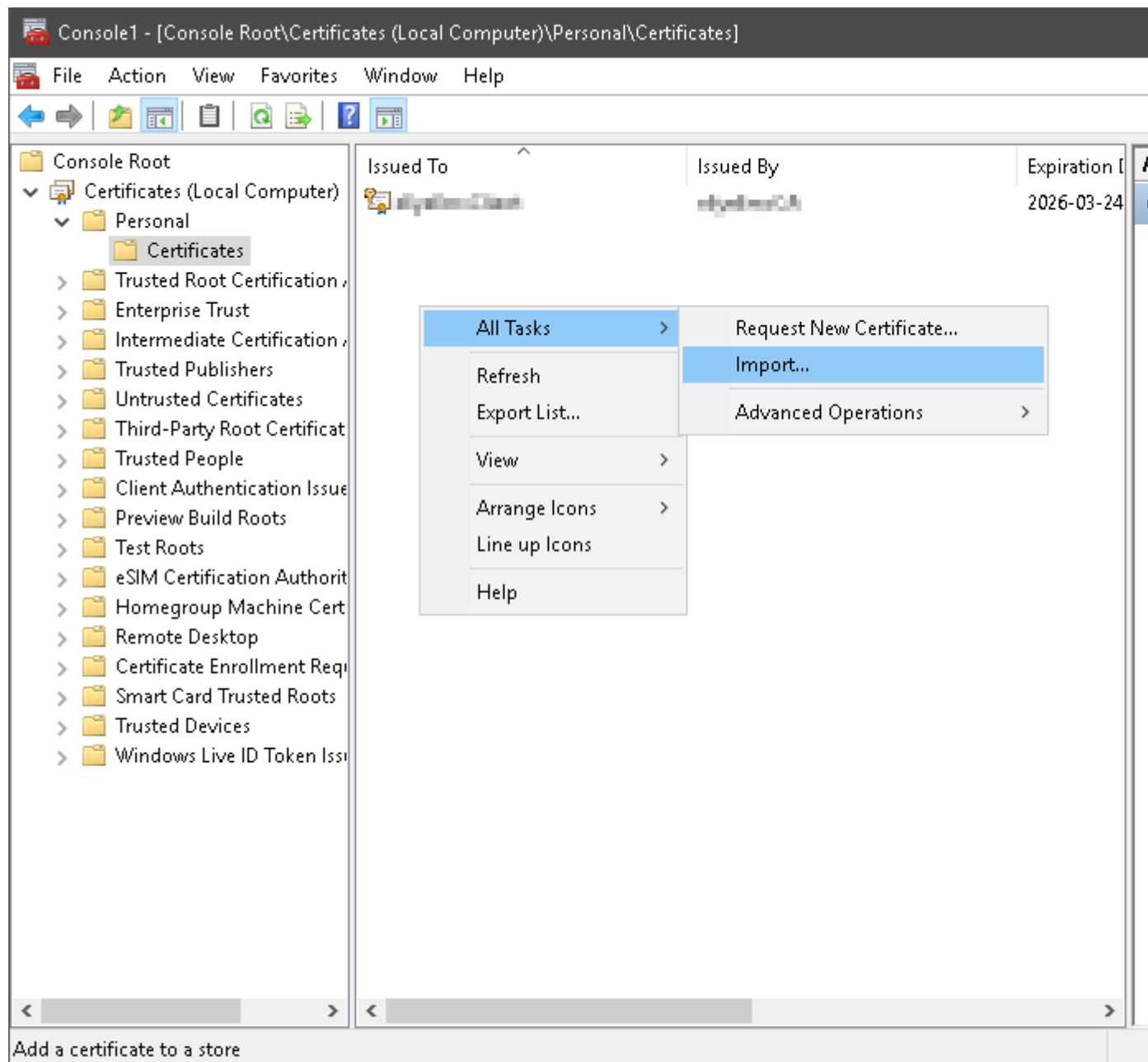
☐ Protect private key using virtualized-based security(Non-exportable)

☒ Include all extended properties.

Next Cancel

Manually importing the client certificate - Windows 10

1. The manual import can be completed using Microsoft Management Console (MMC).
Open Command Prompt and type `mmc` and hit **Enter** to open MMC.
Go to File menu, click **Add/Remove Snap In**, and add the **Certificates** snap-in for **Local Computer**.
Once added, right-click in the middle window and select **All Tasks > Import**.



2. Once imported, the certificate should show up under **Local Computer** and not **Current User**.

Export the FortiAuthenticator certificate and import it under **Trusted Root Certification Authorities**, again under **Certificates (Local Computer)**.