There is a vulnerability in the SecureDoc Windows

SecureDoc Enterprise Server

Comprehensive Guide to Configuring and Deploying TLS Certificates in SDConnex

Published May 24, 2024

SecureDoc by WinMagic

Contents

SecureDoc Support

WinMagic strongly recommends that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and new features.

Please visit Knowledge Base Article 1397 for more information on End of Life and End of Support timelines for SecureDoc software releases.

How to Install/Upgrade

Customers with an active support plan should contact support@winmagic.com to receive the latest download link for their SecureDoc upgrade.

Configuring TLS Certificates for SDConnex Prerequisites and Procedures

TLS Certificate Configuration for SDConnex

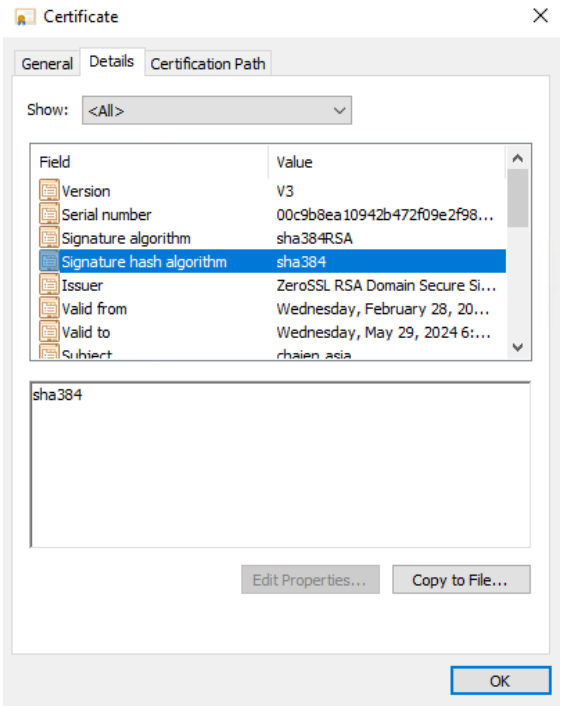
Prerequisites:

- **Hash Algorithm and Key Length:** Ensure the certificate uses a hash algorithm of at least SHA256 and a key length of 2048 bits.
- **Key Usage:** The certificate's "Key Usage" field must include "Digital Signature" and "Key Encipherment".
- **Certificate Formats:** Typically, ".cer" files contain only the public key. To provide the private key required by SDConnex on the server side, the certificate in the OS store should be in ".pfx" or ".p12" format.
- **Exportable Key Option:** When importing the ".pfx" certificate into certmgr.msc, select the option "Mark this key as exportable" to allow future backup or transportation of your key.
- **Including Certificate in Installation Packages**: To include your TLS certificate in new installation packages, import it into SES Global Options via Tools > Options > Server's RSA keys.
- **Server's Certificate Store:** Install the certificate in the server's certificate store.
    - **Optional Profile Settings:** "Validate server certificate" and "Verify host name" are optional in the profile. If these settings are disabled, the installation package can be deployed without requiring the certificate on the client side.
    - Additional information on these settings can be found in the notes section at the bottom of the document.

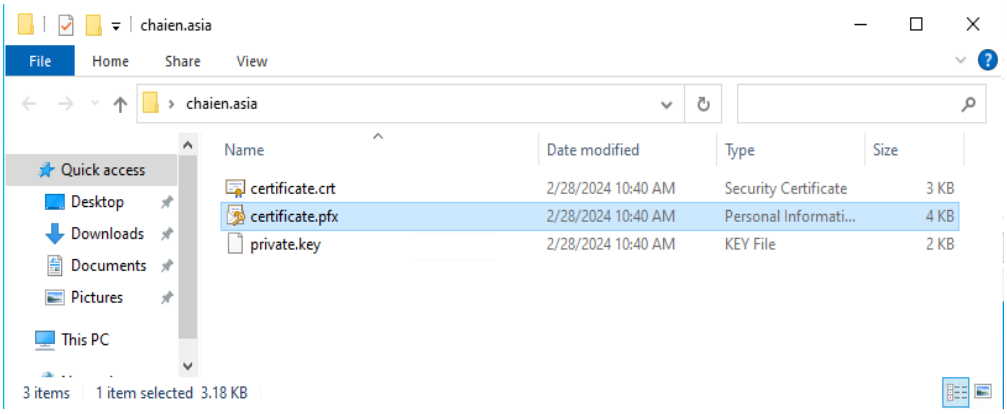
This chapter provides essential guidelines for setting up TLS certificates, ensuring secure communications within SDConnex environments.

Comprehensive Guide to Configuring and Deploying TLS Certificates in SDConnex

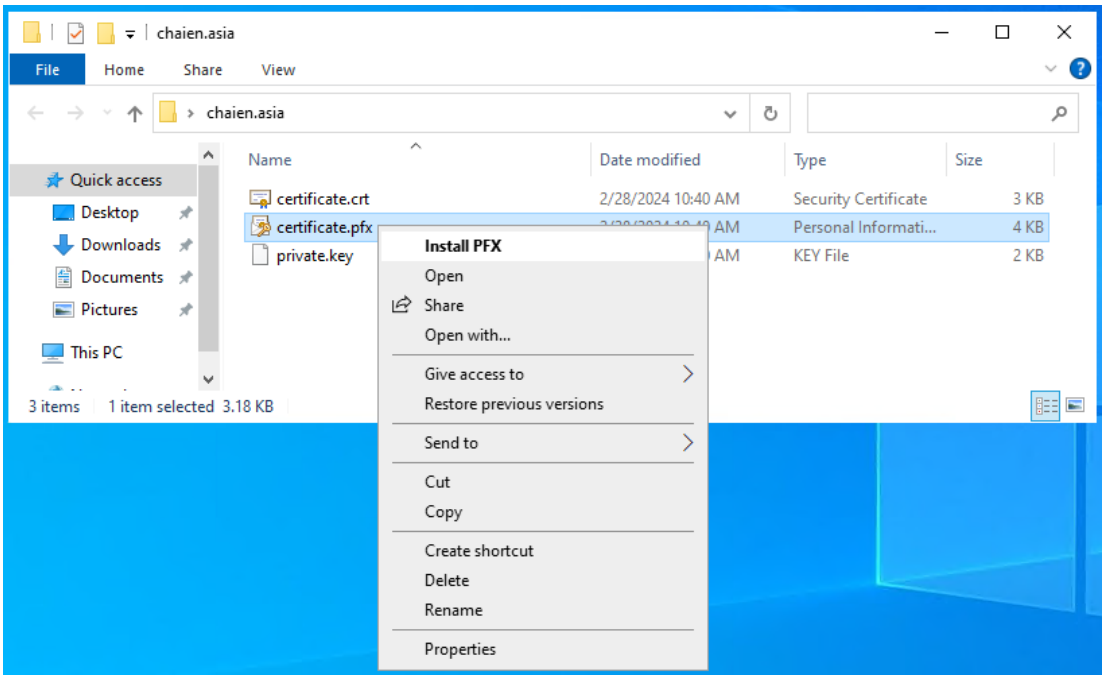
1. Generate a "certificate.crt" and a "private.key" using a SHA384 hash algorithm and a key length of 2048 bits. This process involves creating a public certificate file (certificate.crt) and a private key file (private.key). The SHA384 algorithm provides a strong level of security, ensuring that the certificate and key are robust against cryptographic attacks. The key length of 2048 bits further enhances security, making it difficult for unauthorized entities to decrypt the data. This step is essential for establishing a secure communication channel using TLS in SD Connex.



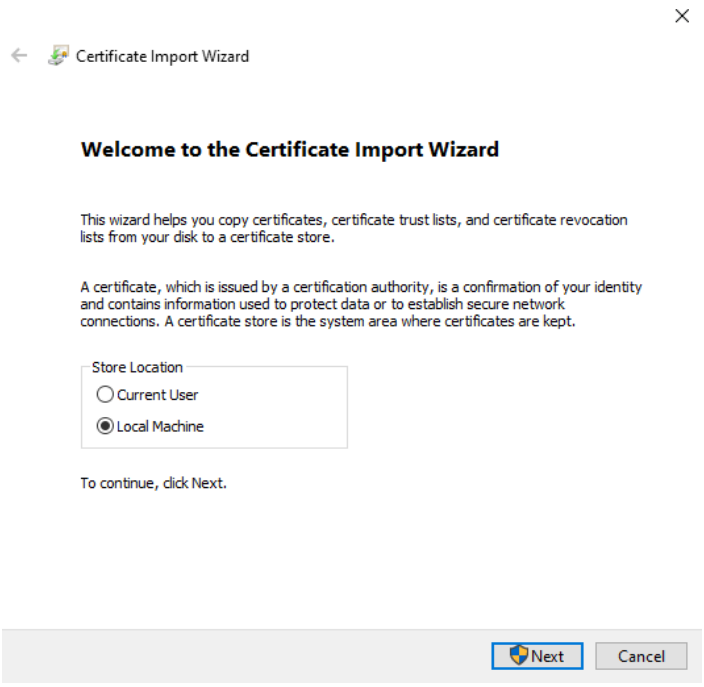
2. Convert both the "certificate.crt" and the "private.key" files to the PKCS#12/PFX format. This format combines the certificate and the private key into a single file, ensuring secure and efficient management and transfer of the cryptographic material.



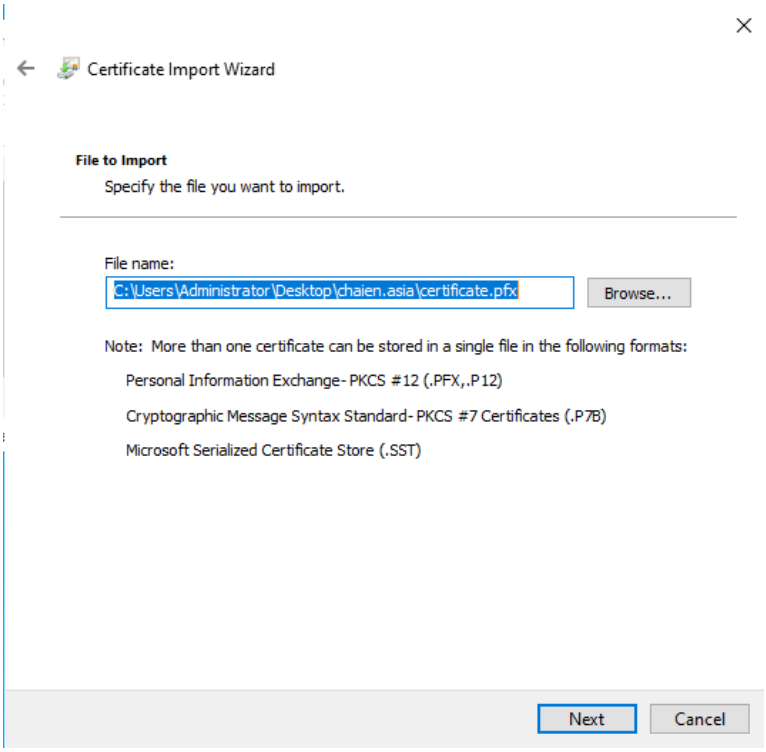
3. Install "***Certificate.pfx***".



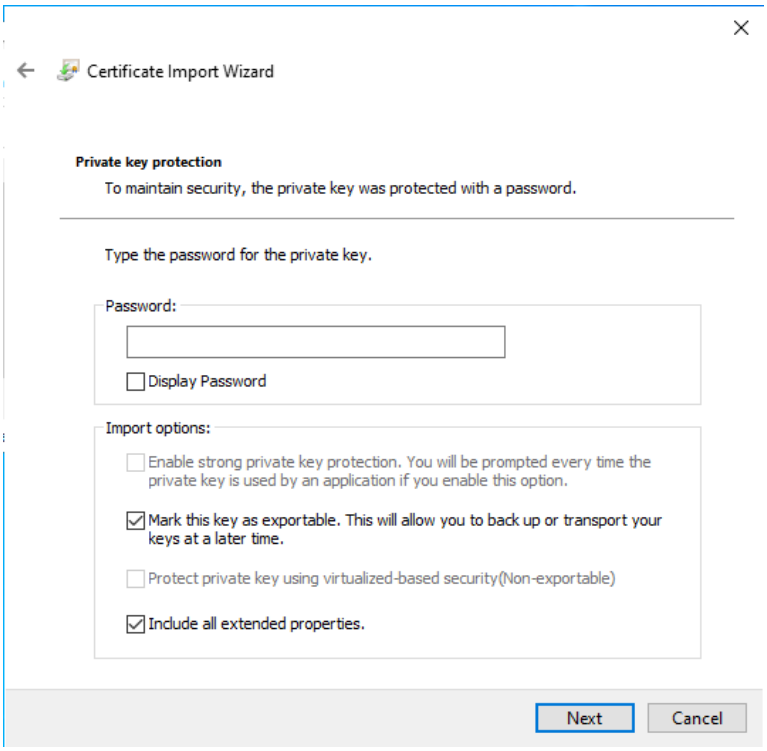
4. Select "***Local machine***" and "***Next***".



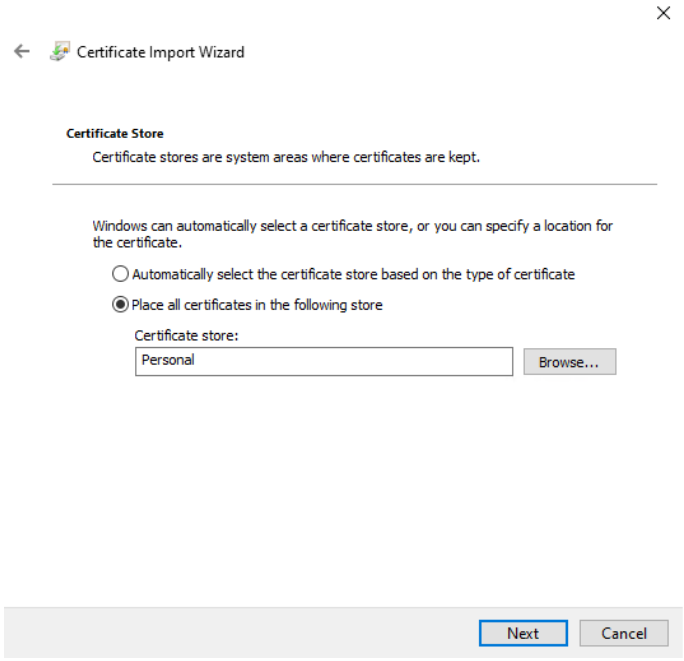
5. Click "***Next***".



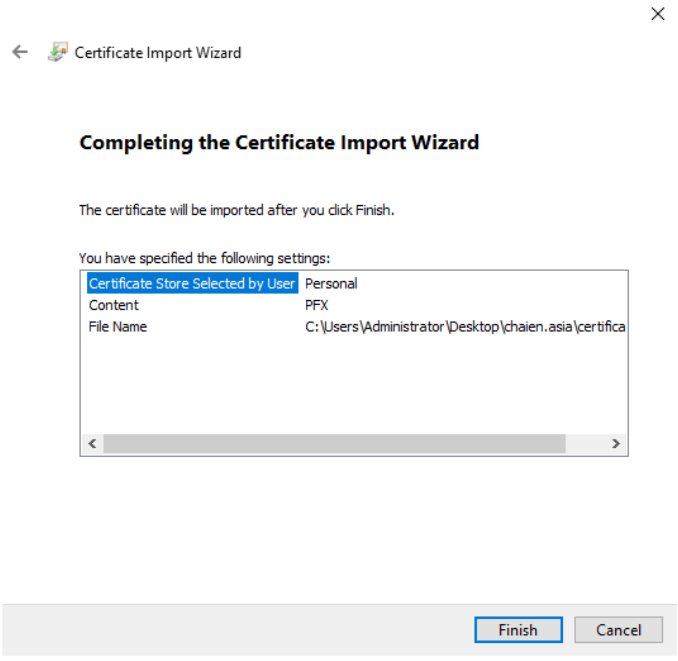
6. Enter the password and check "***Mark this key as exportable. This will allow you to back up or transport your key at a later time***", then click "***Next***".



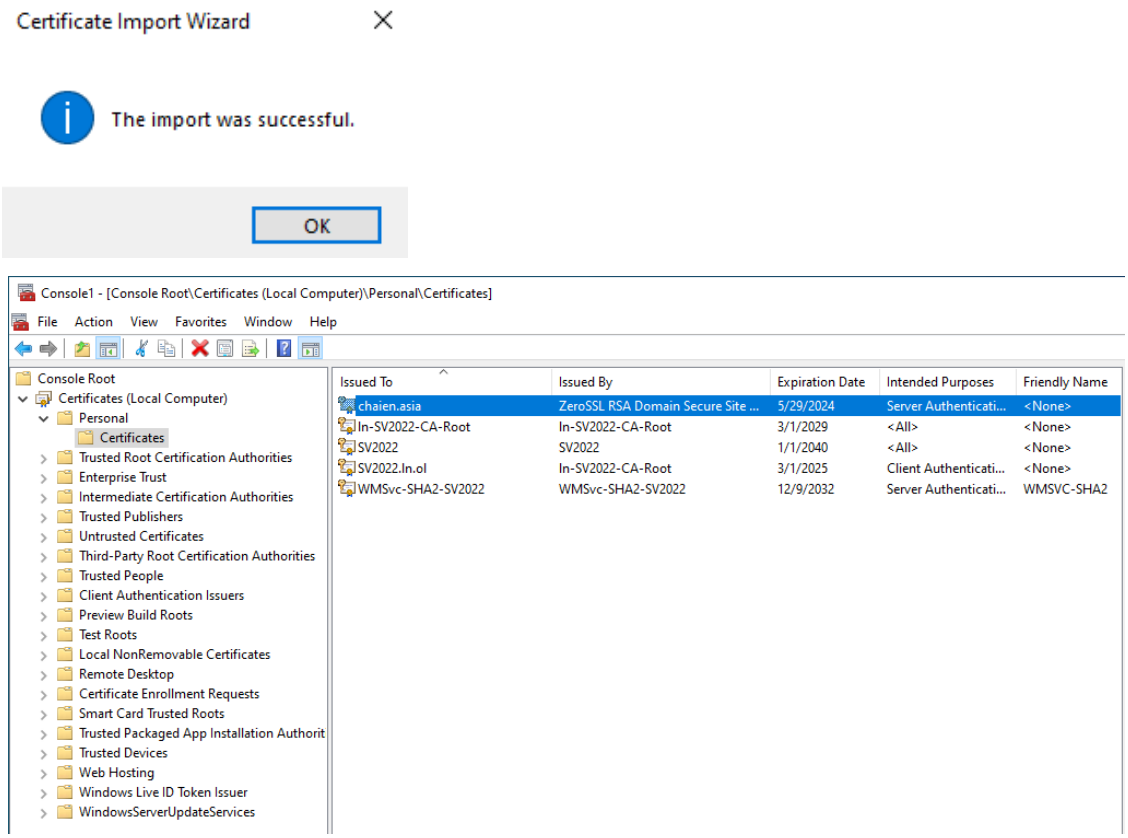
7. Select “Place all certificates in the following store” to specify where the certificate should be stored. Then, click "Browse" to open the list of available certificate stores. Navigate to and select the "Personal" certificate store. This ensures that the certificate is placed in the appropriate store for use by the local machine.



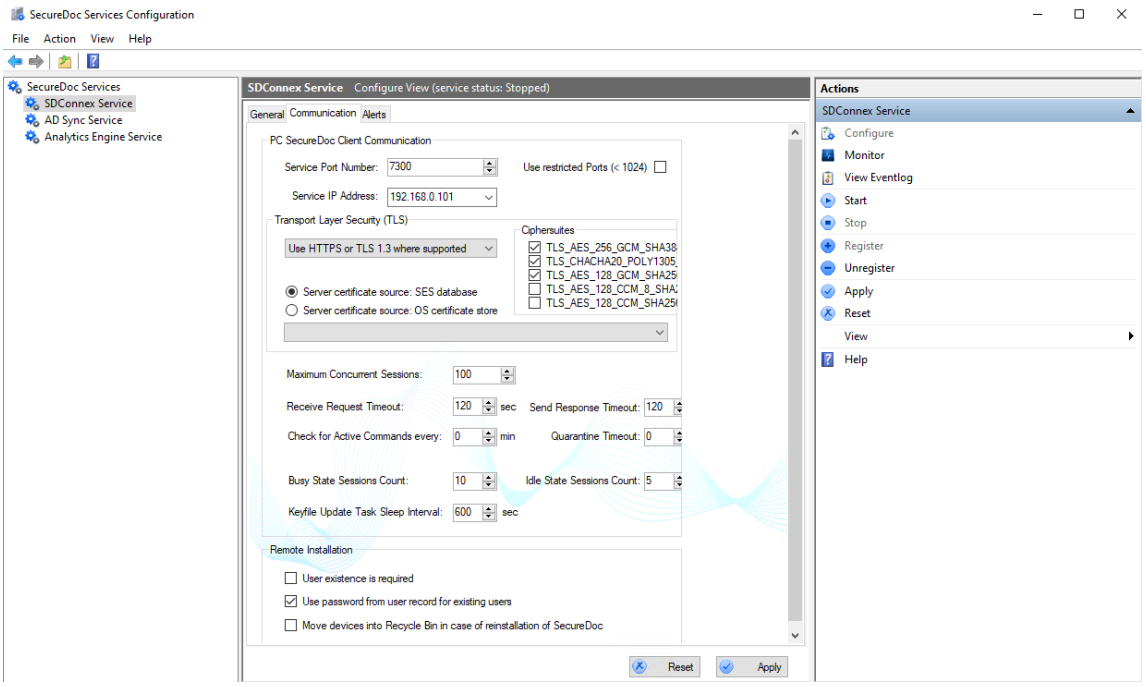
8. Click “Finish”.



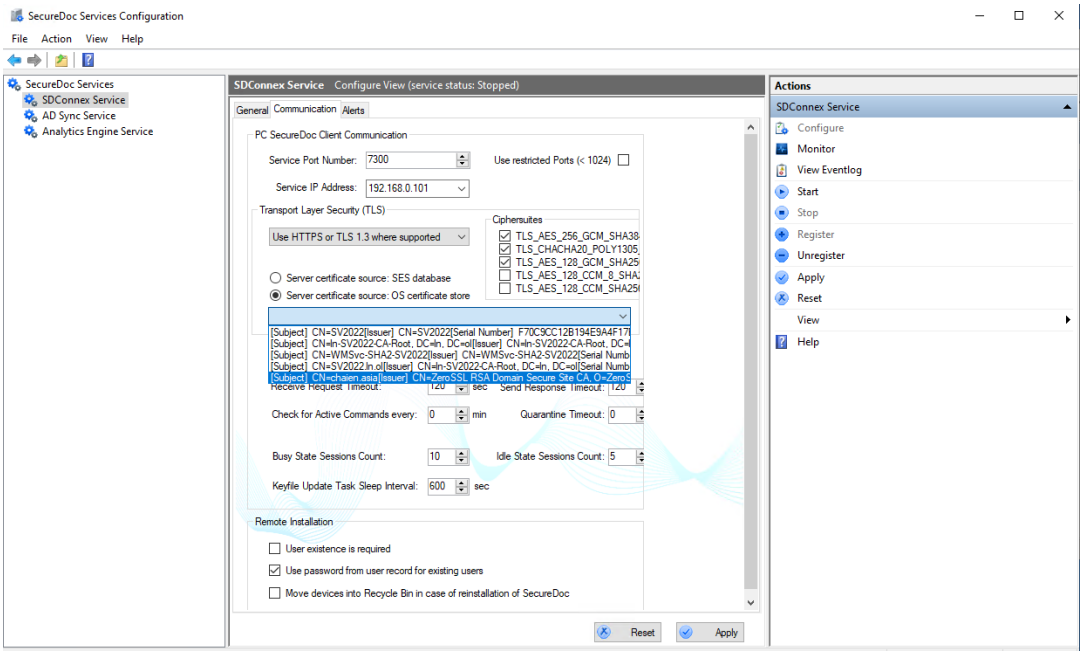
9. Successful.



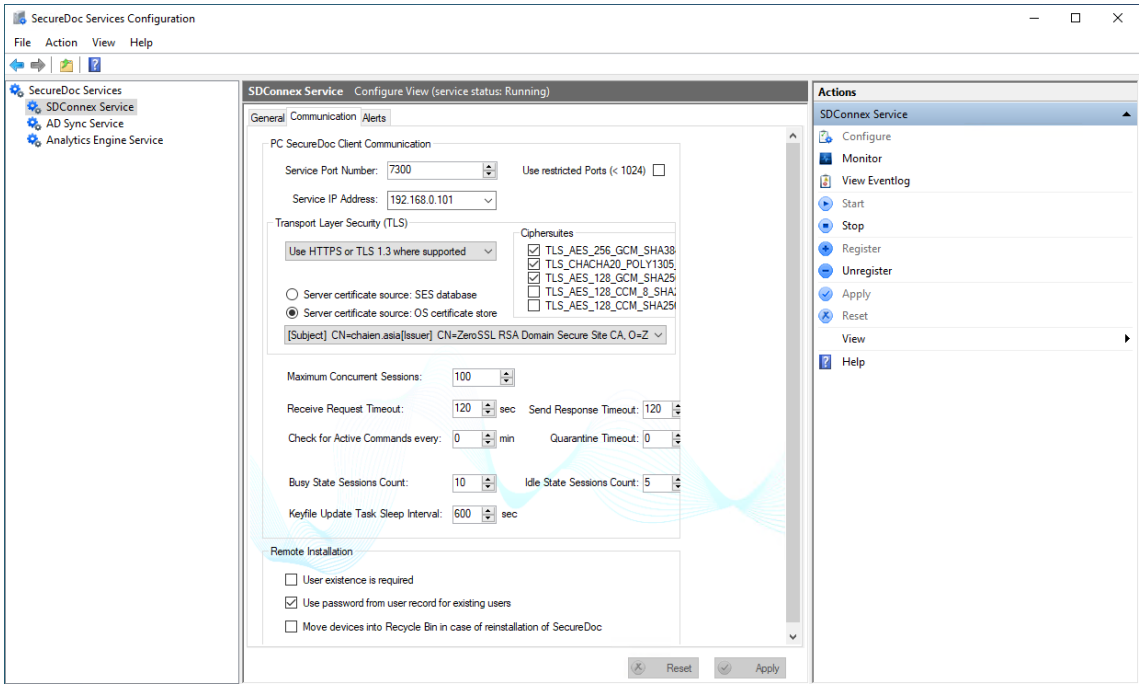
10. Run "***SecureDoc Services Configuration***".



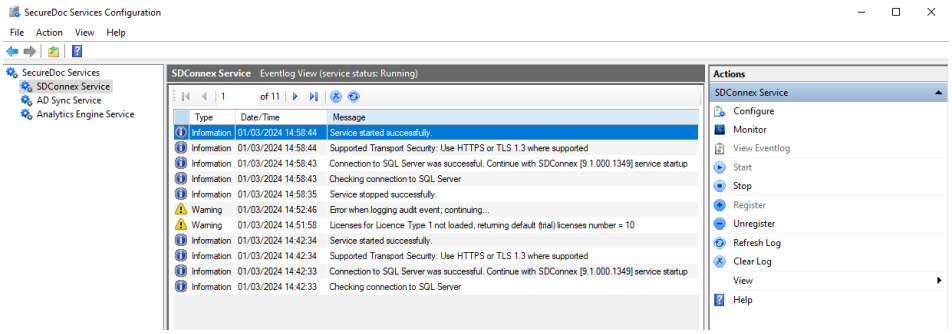
11. Select "***Server certificate source: OS certificate store***" and your imported certificate.



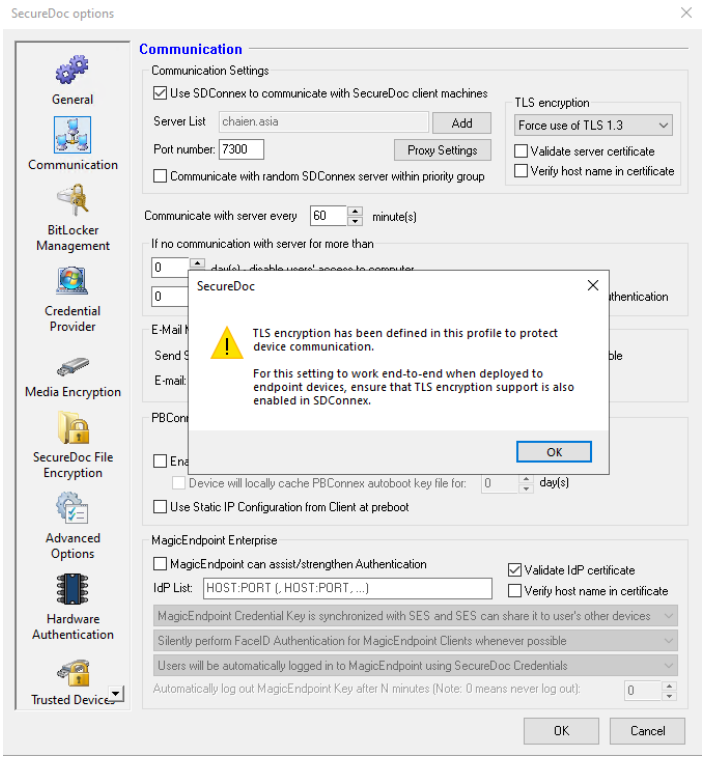
12. Click "***Apply***" and "***Start***" → Service status: Running successfully.



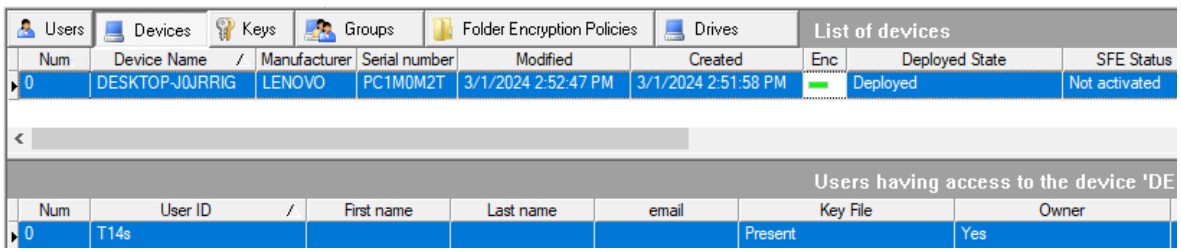
13. Verify the installation by selecting "View EventLog" to ensure there are no errors or warnings.



14. Create an SD Profile and, in the “Communication” tab, select TLS encryption as either “Force use of TLS 1.3” or “HTTPS”.
    In this example, the “Validate server certificate” and “Verify host name” options are disabled. Refer to the “Notes” section at the bottom of the document for guidance on these settings.



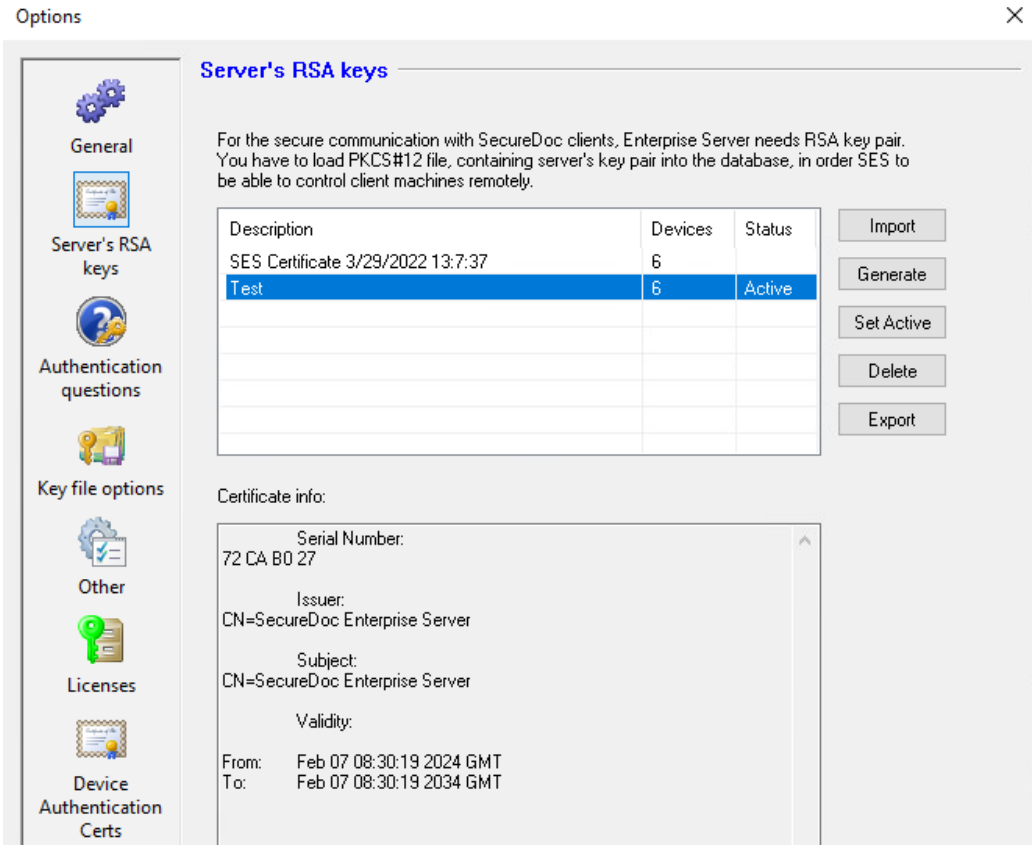
15. Successfully deploy the SD package to the client. BootLogon will be installed, and the hard drive will be encrypted as expected.



Notes:

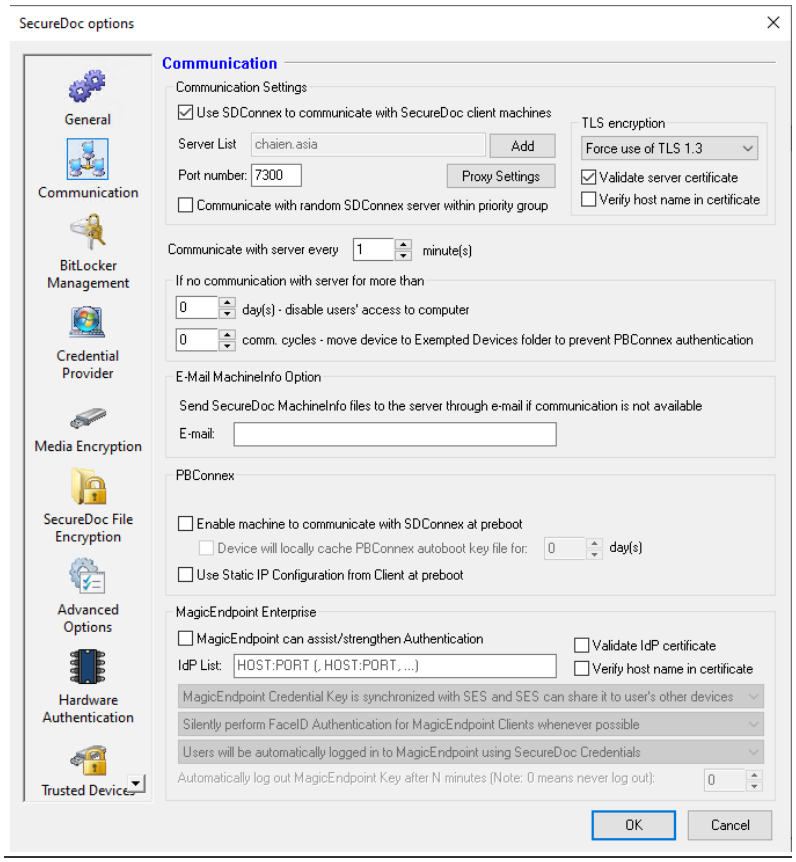
If you want to include your own TLS certificate in new installation packages, you must import the certificate into the SES Global Options. To do this, follow these steps:

- Open the SES Global Options by navigating to Tools > Options.
- Select the "Server's RSA keys" section.
- Import your TLS certificate into this section, ensuring it is properly configured and set to be used in the new installation packages.
- This step ensures that the TLS certificate will be included in the installation packages, facilitating secure communication and encryption protocols during the deployment process.



- ***"Validate server certificate"*** *and* ***"Verify host name"*** are both optional settings in the profile. If they are disabled, then no extra steps need to be done on the client side. The installation package can be installed without installing the certificate on the client side.

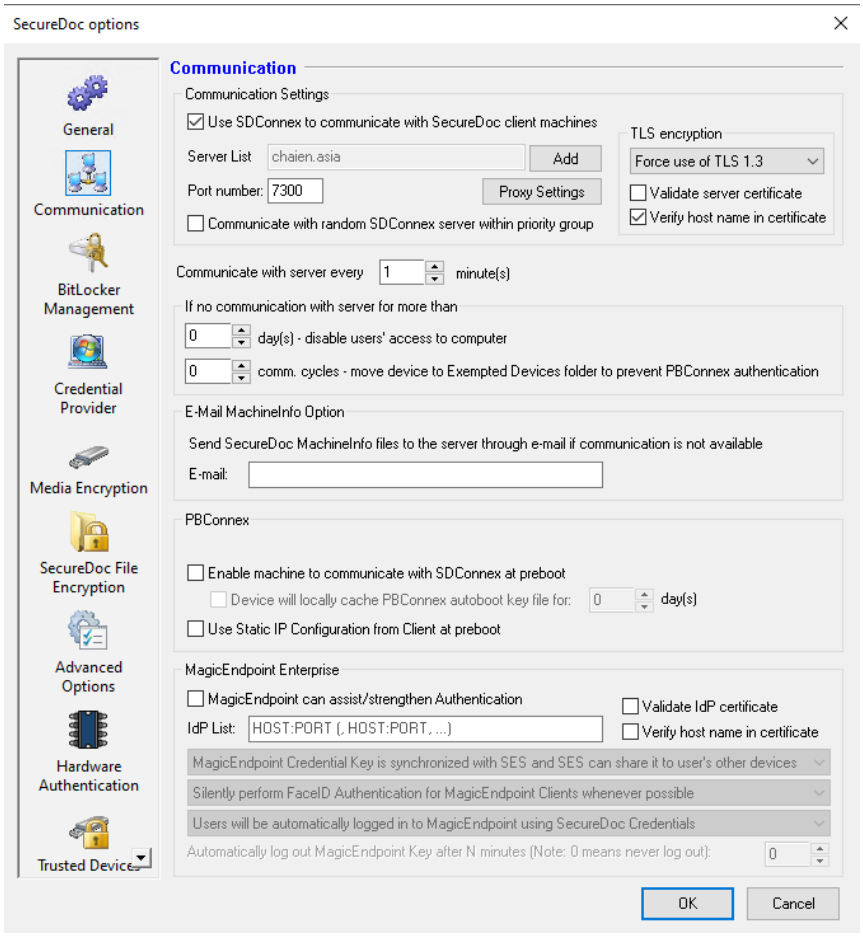
  a. Enable "*Validate server certificate*" in profile:



- Ensure the selected certificate in SDConnex matches the intended TLS certificate.
- Create a new SD package.
- Before deploying the SD package on the client device, install the TLS certificate used in SDConnex on the device. To do this, go to Install Certificate > Local Machine > Trusted Root Certificate Authorities.

Note: The certificate included in installation packages is the one marked as 'Active' in the SES Global Options. If the SDConnex TLS certificate differs from the one in Global Options, you must distribute the SDConnex TLS certificate to the device through other means and install it.

b. Enable "***Verify host name in certificate***":



- Ensure the SDConnex name matches the certificate name.
- Verify that this certificate is selected in SDConnex.
- Create a new SD package.
- Before deploying the SD package on the client device, install the TLS certificate used in SDConnex on the device. Navigate to Install Certificate > Local Machine > Trusted Root Certificate Authorities.

Note: The certificate included in installation packages is the one marked as 'Active' in the SES Global Options. If the SDConnex TLS certificate is different from the one in Global Options, you must distribute the SDConnex TLS certificate to the device through other means and install it.

Conclusion and Key Takeaways for TLS Certificate Deployment in SDConnex

This guide provides detailed instructions for configuring and deploying TLS certificates in SDConnex, ensuring secure communication within the system. The process begins with generating a certificate and key using a robust hash algorithm and key length, followed by converting these to the PKCS#12/PFX format for secure management. The certificate is then installed, configured in the SecureDoc Services, and verified through event logs to ensure error-free operation.

Key steps include creating an SD Profile with appropriate TLS encryption settings and deploying the SD package to client devices, ensuring BootLogon installation and hard drive encryption. Additionally, the guide covers optional settings for validating the server certificate and verifying the hostname, offering flexibility in deployment while balancing security considerations.

For those who wish to include their TLS certificates in new installation packages, the guide explains how to import the certificate into SES Global Options, ensuring it is used during deployment. By following these comprehensive steps, administrators can achieve a secure and efficient TLS certificate deployment in SDConnex environments.

Contact WinMagic

WinMagic		Sales:	sales@winmagic.com
5770 Hurontario Street, Suite 501		Marketing:	marketing@winmagic.com
Mississauga, Ontario, L5R 3G5		Human Resources:	hr@winmagic.com
Toll free: 1-888-879-5879		Technical Support:	support@winmagic.com
Phone: (905) 502-7000		For information:	info@winmagic.com
Fax: (905) 502-7001		For billing inquiries:	finance@winmagic.com

Acknowledgements

This product includes cryptographic software written by Antoon Bosselaers, Hans Dobbertin, Bart Preneel, Eric Young (eay@mincom.oz.au) and Joan Daemen and Vincent Rijmen, creators of the Rijndael AES algorithm.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.OpenSSL.org/).

WinMagic would like to thank these developers for their software contributions.

Printed in Canada Many products, software and technologies are subject to export control for both Canada and the United States of America. WinMagic advises all customers that they are responsible for familiarizing themselves with these regulations. Exports and re-exports of WinMagic Inc. products are subject to Canadian and US export controls administered by the Canadian Border Services Agency (CBSA) and the Commerce Department's Bureau of Industry and Security (BIS). For more information, visit WinMagic's web site or the web site of the appropriate agency.