Wildcard Certificates

Importing PKCS#12 and .PFX files

Important: GoPrint requires the certificate chain password to be trustno1

When importing certificates into the Java Keystore generated on another certificate store typically Wildcard certificates, the private key must also be included. The process includes exporting the certificate and its trusted certificates along with the private key in a PKCS#12 format or .PFX for Windows.

GoPrint provides the built-in TLS import Tool to import your PKCS#12/PFX file or you can use the Java Keytool from a command line to generate a new keystore and import the certificate.

Important: The TLS import tool imports your cert directly into the existing gtx.keystore file. It's important to backup your current GS4\gtx.keystore file and restore if errors occur.

Personal Information Exchange Overview (PKCS #12)

The Personal Information Exchange format (PFX, also called PKCS #12) supports secure storage of certificates, private keys, and all certificates in a certification path.

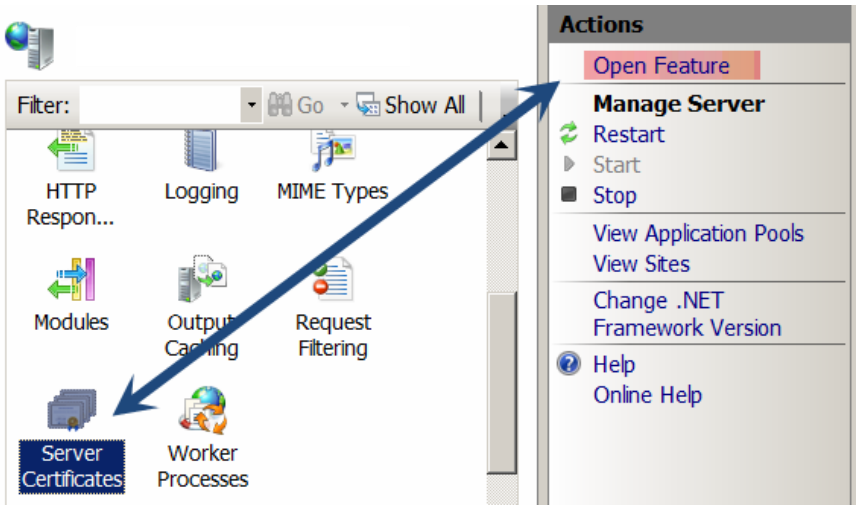
The PKCS #12 file format is the only file format that can be used to export a certificate and its private key.

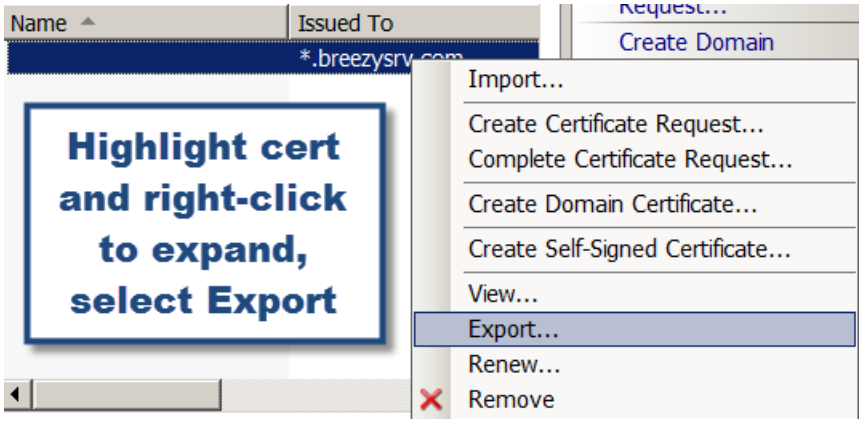
Changing the keystore Password
GoPrint requires a default keystore password of trustno1. If you receive a .PFX file with a different password, you must import the .PFX into the local windows certificate store and then Export the keypair, (all certificates in the path) and secure with a new password of trustno1. See Page 32.

Keypair
1. Public key
2. Private key
3. Intermediate certificate
4. Root Certificate

HOW IT WORKS!

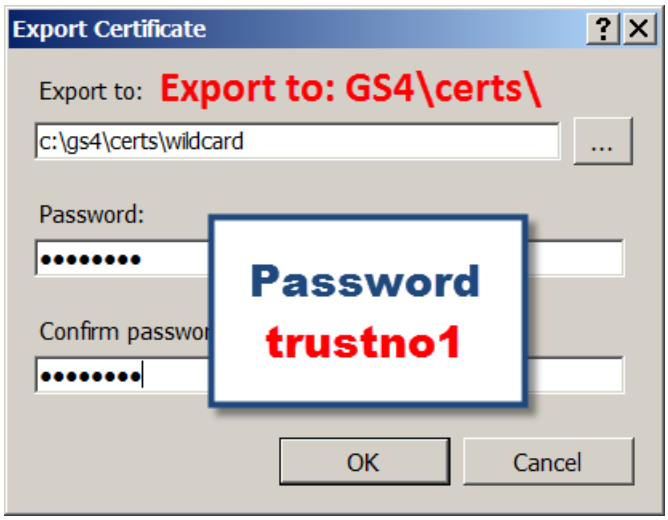
Example: If the certificate reply was created in the Windows certificate store, then the certificate chain and private key may be exported.





Important: a password is required to protect the key. If requesting the file from a staff member it's important to obtain the password. To import seamlessly with GoPrint, it's important to request a password of "**trustno1"**

If you did not receive your certificate with this password then skip to page 32 to learn how to change it.

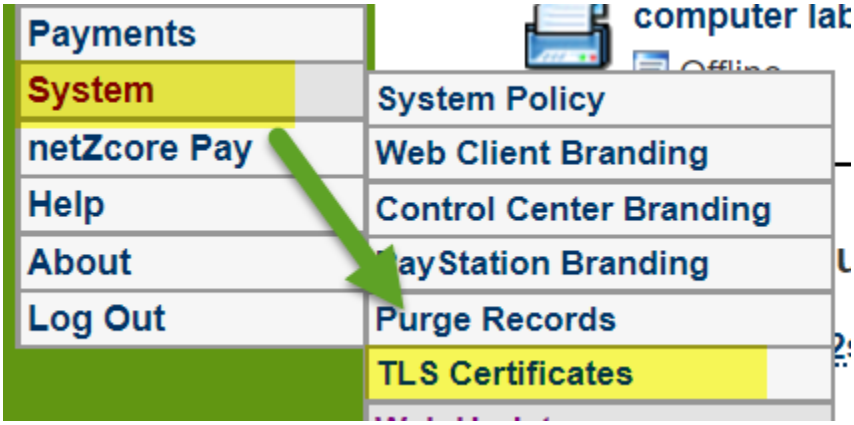


Control Center Certificate Import Tool

GoPrint provides the TLS Import tool to allow you to quickly and painlessly import your certificate. Optionally, if the import is unsuccessful, you can use the Java Keytool command to generate a new keystore and import the .pfx file. See instructions below.

Important: The TLS import tool imports your cert directly into the existing gtx.keystore file. Backup your current GS4\gtx.keystore file and restore it if errors occur. Optionally, you can delete the new keystore and restart the GS4 Services and a new default gtx.keystore gets created.

Step 1 – Navigate to System – TLS Certificates



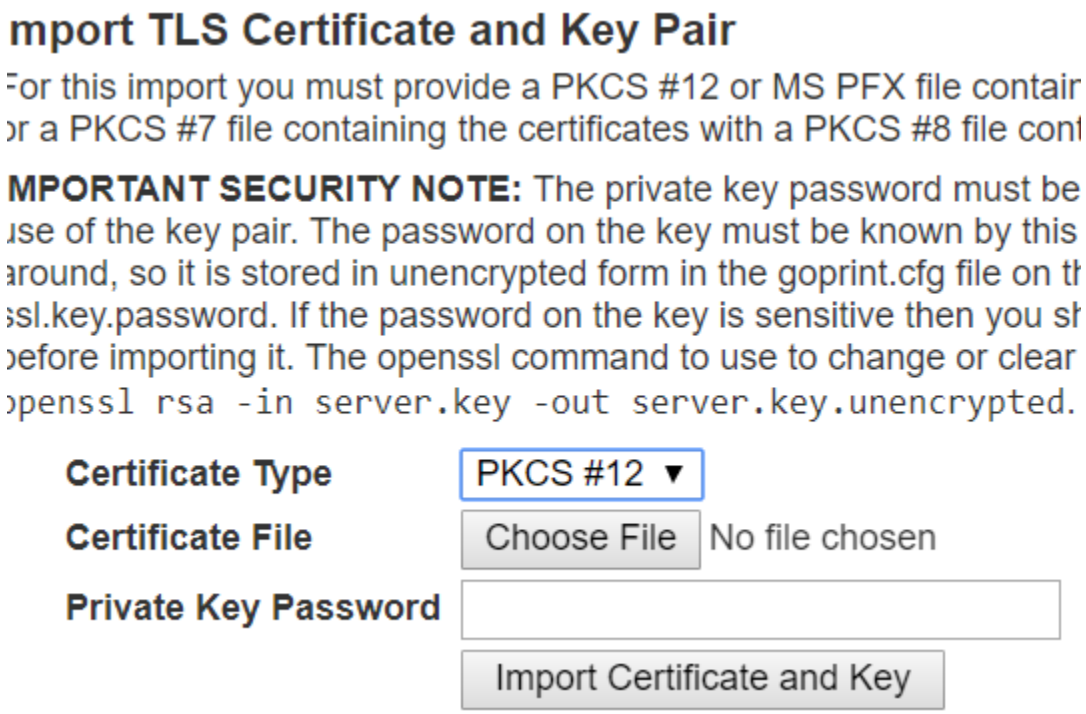
1. Scroll down to Import TLS Certificate and Key Pair and select

If you created the TLS certificate and key pair for this server somewhere else, such as by using the openssl utility, or if your organization has a wildcard TLS certificate you don't need to generate a public/private key pair for this server, since multiple servers on your network share the same TLS certificate and the same public/private key pair. Instead, import your organization's signed wildcard TLS certificate and public/private key along with any intermediate root certificates.

Import TLS Certificate and Key Pair

Import an existing TLS certificate and public/private key pair that has already been issued for that public key.

2. Certificate file: browse to the PKCS #12 file representing the private key.
3. Choose the .pfx
4. Private Key Password: trustno1 (created when you exported the .pfx file)
5. Restart the GS4-Services



If no errors exist, you have successfully imported your .pfx file. See troubleshooting for errors.

Important: Ensure that all web client popups now reference the FQDN as noted in the SSL certificate.

Change the goprint.cfg file on the GTX server and any remote Agents to reference the FQDN

Restart the G4 Services

Test the new keystore

Open the Web Client Popup or Control Center using a secure https port. If not prompted to trust the certificate, then the KeyStore has successfully been generated.

Java Keytool option

Step 1 – Create a new blank Key Store

```
keytool -importkeystore -destkeystore c:\gs4\certs\gtx.keystore -
deststorepass trustno1 -srckeystore c:\gs4\certs\wildcard.pfx -
srcstoretype PKCS12 -srcstorepass trustno1
```

```
C:\GS4\jre\bin>keytool -importkeystore -destkeystore c:\gs4\certs\gtx.keystore -
deststorepass trustno1 -srckeystore c:\gs4\certs\wildcard.pfx -srcstoretype PKCS
12 -srcstorepass trustno1
Entry for alias le-72d11884-bbab-4d4d-a79f-b5f3072a715e successfully imported.
Import command completed:  1 entries successfully imported, 0 entries failed or
cancelled
```

The PKCS#12 was successfully imported and the new gtx.keystore created!!!

```
Entry for alias le-72d11884-bbab-4d4d-a79f-b5f3072a715e
successfully imported. Import command completed:     1 entries
successfully imported, 0 entries failed or cancelled
```

Step 2 - Change the default Alias to goprintservercert

The Goprint system requires a Keystore alias name of 'goprintservercert' and by default the importkeystore command generates a generic alias, as highlighted below:

```
Entry for alias le-72d11884-bbab-4d4d-a79f-b5f3072a715e
successfully imported. Import command completed:     1 entries
successfully imported, 0 entries failed or cancelled
```


Issue the command:

```
keytool -changealias -alias le-72d11884-bbab-4d4d-a79f-b5f3072a715e
-destalias goprintservercert -keystore c:\gs4\certs\gtx.keystore
```

```
C:\GS4\jre\bin>keytool -changealias -alias le-72d11884-bbab-4d4d-a79f-b5f3072a715e -de
stalias goprintservercert -keystore c:\gs4\certs\gtx.keystore
Enter keystore password:
```

Step 3 - view the contents of the Keystore to confirm the alias change

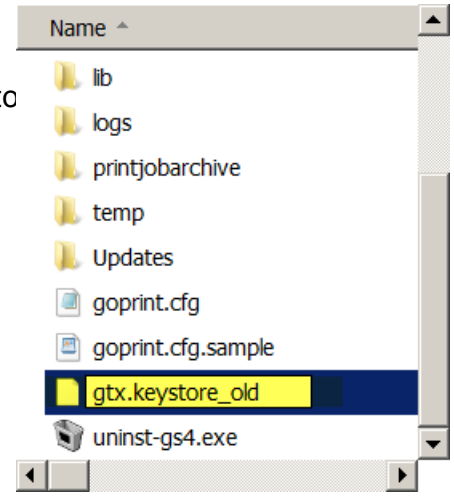
Issue command:

C:\GS4\jre\bin>keytool -v -list -keystore
c:\gs4\certs\gtx.keystore Enter keystore password:

```
C:\GS4\jre\bin>keytool -v -list -keystore c:\gs4\certs\gtx.keystore
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: goprintservercert
Creation date: Oct 17, 2013
```

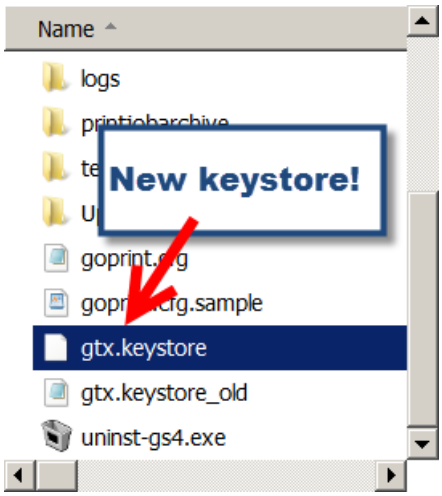
Step 4 - Backup the current gtx.keystore

The current gtx.keystore is found under the GS4\ root directo

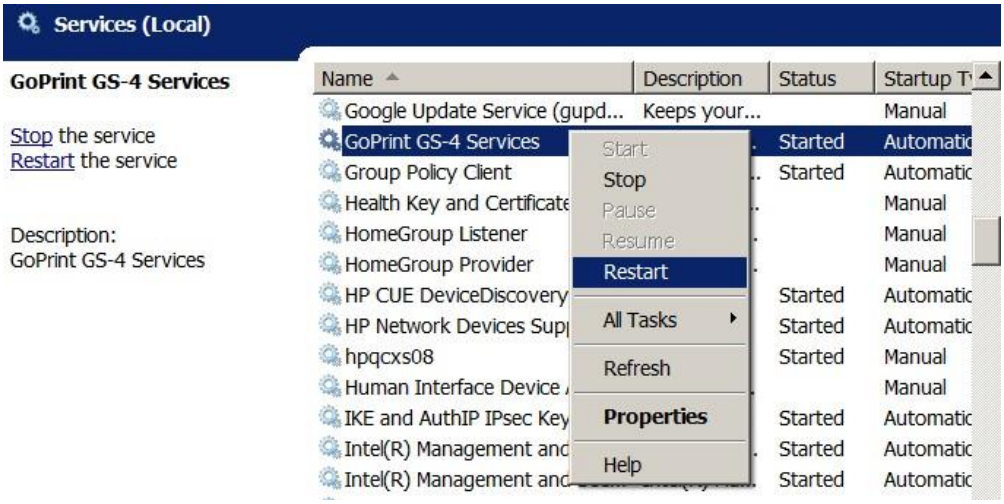


Step 5 – Replace with the new Keystore

Copy and paste the new gtx.keystore to the GS4 directory

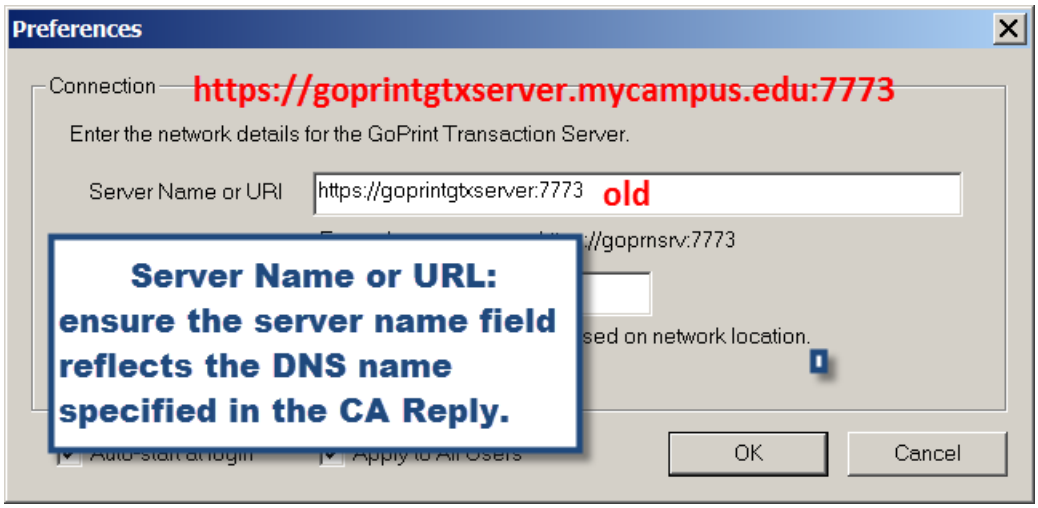


Step 6 – Restart the GoPrint GS-4 Services



Step 7 – ensure web client profiles reflect the FQDN name specified in the CA Reply

If the Web Client popup was installed using the hostname of the GTX server then in order to apply the SSL certificate the Web Client preference setting must be updated.



Step 8 – make a backup of your new gtx.keystore file and certificate files and save in a secure place from the server!

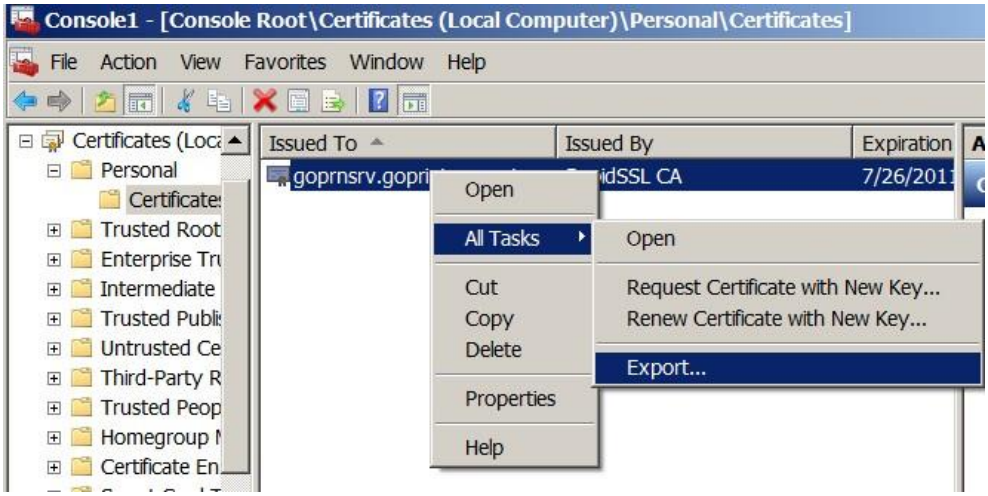
Changing the Exported PKCS#12 (.PFX) Password

If you receive the incorrect password!

When exporting a certificate chain from a certificate store you're required to create a password. GoPrint requires the password of 'trustno1'. If your administrator did not create this password, then you will need to import it into the Local Certificate Store and Export it where you can then change the password.

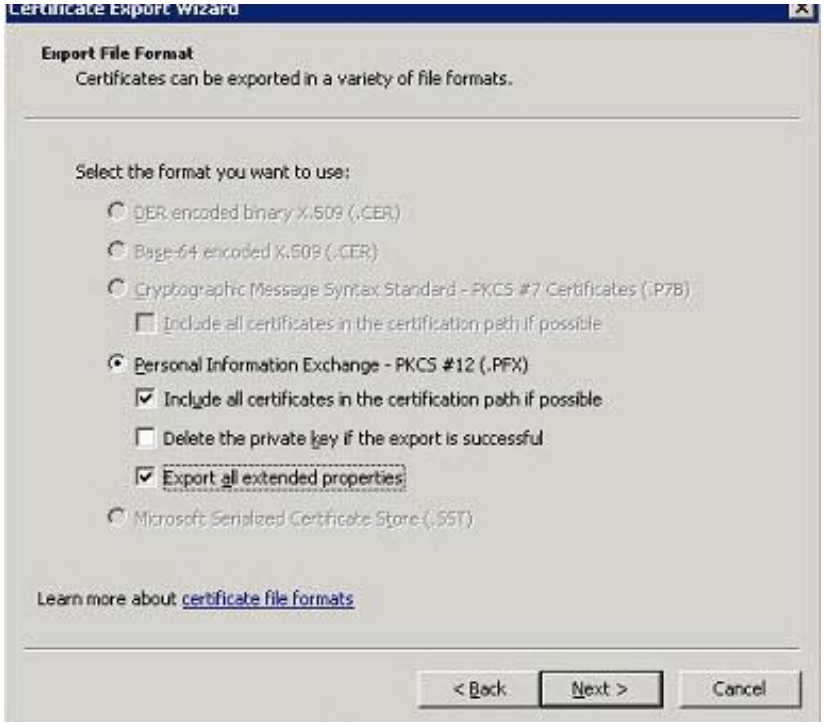
Exporting a Windows Certificate Chain

1. Open the Certificate Store where certificate chain was imported.
2. Highlight your certificate and right-click, select All Tasks - Export



3. Select the Personal Information Exchange – PKCS#12 (.PFX) radio button

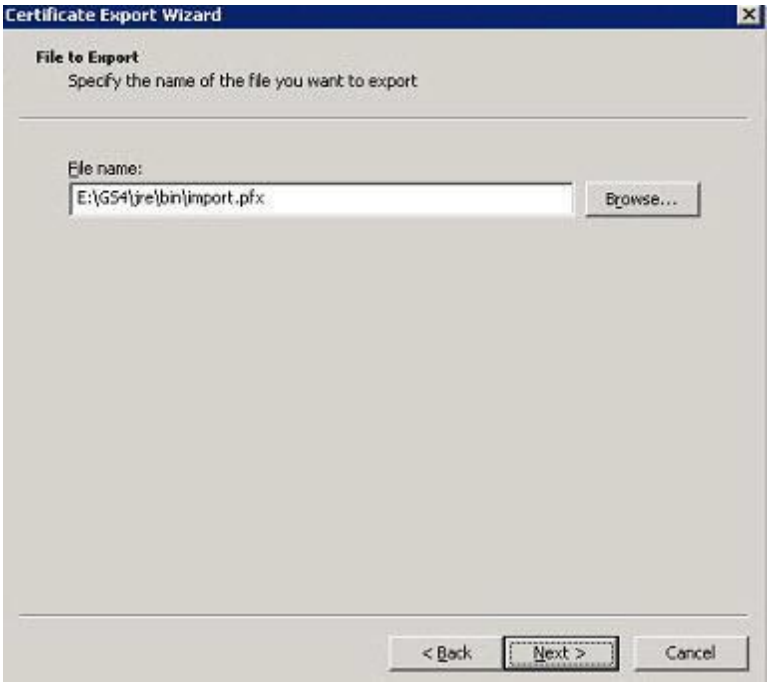
- Check the "Include all certificates in the certificate path if possible" radio button
- Check Export all extended properties.
- Select Next



4. Select Yes, export the private Key and click Next

5. Enter a File name and desired path and click Next

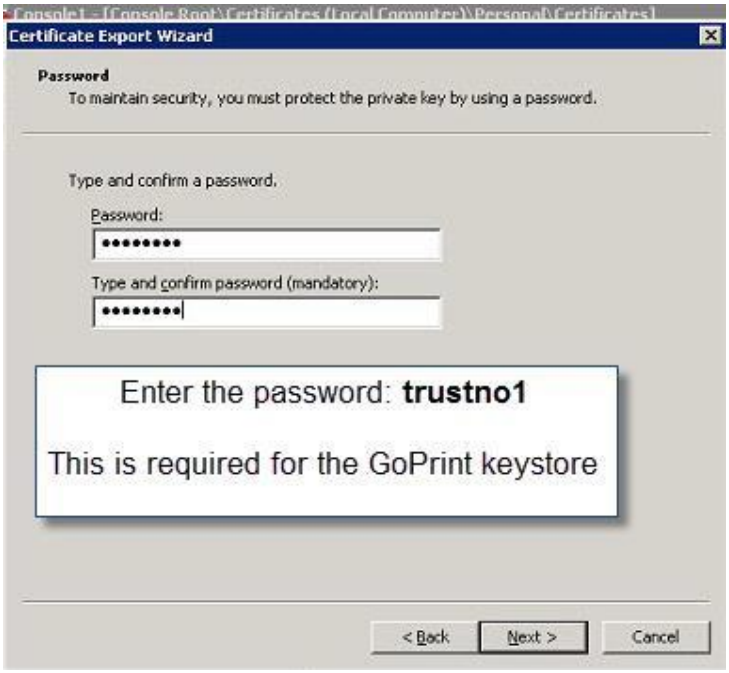
   Note: It's recommended to save the file under the GS4\certs directory



6. Create a password of trustno1 (this is the same password required to use when creating the Java keystone and MUST match.

Important: this MUST be the same password used by the GoPrint Keystore

DO NOT use another password!



Completing the Certificate Export Wizard appears:

7. Click Finish

8. Follow the previous steps to import your certificate into the Java

Troubleshooting SSL Errors

Error: After restarting the GoPrint GS-4 Services, the CPU races up to 100% and Task Manager displays the Java process racing. This is an indication the keystore has been improperly formatted.

Solution: This scenario occurs when the Private Key was generated on another server and does not exist in the Java keystore. To solve, see the instructions on how to import a Private Key in the document; "Advanced_SSL_Certificates.pdf

Error: keytool error**:** java.lang.Exception: Input not an X.509 certificate

```
Keytool -import -trustcacerts -alias server -file goprnsrv_goprintsupport_com.p7b -
keystore keystore
```

Solution: the alias name was incorrect, it should be goprintservercert

Or

```
keytool -import -trustcacerts -alias goprintservercert -file
goprnsrv_goprintsupport_com.p7b -keystore keystores
```

Solution: the keystore name is incorrect, is should keystore not keystores

Error: keytool error: java.lang.Exception: Certificate reply does not contain public key for <goprintservercert>

Solution: The CA Reply file is tied to the public key of another keystore. When a new keystore and keypair are created, you cannot use the CA reply generated from another keystore. When issues occur, you must generate a new keystore and keypair and submit a new CSR to the CA and import the updated CA reply.

Error: keytool error: java.lang.RuntimeException: Usage error, goprnsrv_goprint_com.p7b is not a legal command

```
keytool -import -trustcacerts -alias goprintservercert-file goprnsrv_goprint_com.p7b -
keystore keystore
```

Solution: Typo, a space needs be entered before the –file switch.

Error: keytool error: java.lang.Exception: Failed to establish chain from reply

```
keytool -import -trustcacerts -alias goprintservercert -file ssl.crt -keystore
keystore
```

Solution: attempting to import the CA First, intermediate has to go first.

```
keytool -import -trustcacerts -alias goprintservercert -file intermediate.crt -
keystore keystore
```

Error: keytool error: java.lang.Exception: Public keys in reply and keystore don't match

Solution: When importing individually, each certificate in the chain must have its own Alias, and only the returned certificate can be imported into the –Alias goprintservercert

```
keytool -import -trustcacerts -alias inter -file intermediate.crt -keystore keystore
-storepass trustno1

Certificate was added to keystore
```

```
c:\GS4\jre\bin>keytool -importkeystore -destkeystore c:\gs4\certs\gtx.keystore
-deststorepass trustno1 -srckeystore c:\gs4\certs\newcert.pfx -srcstoretype
PKCS12 -srcstorepass trustno1
keytool error: java.lang.NullPointerException
```

A **NullPointerException** occurs when using **keytool** to create a CSR file. Description: ... If the message "**keytool error**:**java**.**lang**.**NullPointerException**" occurs after the prompt "Enter keystore password:", the most likely cause of the **error** is entering an empty password value

Java Keytool Basic Commands

View the contents of a Keystore

```
c:\GS4\jre\bin>keytool -list -v -keystore gtx.keystore
```

Handling Nested Domain Names

Anything that has a sub2 level in it is going to be nested and is NOT covered by the wildcard by default.

Example: sub1.domain.com vs. sub2.sub1.domain.com

Hint: A nested subdomain is a subdomain that is deeper than one level:

To fix it for that specific name, you need to add it as a SAN name on the certificate.

1. Create a new GoPrint CSR using the instructions followed previously.
2. Visit your Certification Authorities support site and follow their instructions:

Example: http://www.digicert.com/ssl-support/wildcard-san-names.htm

1. Log into your account, select the order number, click on 'Get a Duplicate', Paste the new CSR, then specify the name in the SAN field

Note: SAN names are just additional names secured by the certificate.

Miscellaneous Topics

Moving a Certificate from Apache to a Java Keystore

1. Backup your certificate:

   To import your certificate to Windows, you will first need to combine your primary certificate, Intermediate (CA) Certificate, and your private key file into a .pfx type backup file. To do this, use the following command:

   ```
   openssl pkcs12 -export -out MyCertBackup.pfx -inkey
   your_private_key_file.txt -in your_domain_name.crt -certfile
   MyCertCA.crt
   ```

This creates a backup of your primary certificate called MyCertBackup.pfx. Copy this file to your GoPrint Windows Server.

Once the .pfx file is copied to your Windows server, follow these instructions to Convert and import your PFX file into a Java KeyStore.