

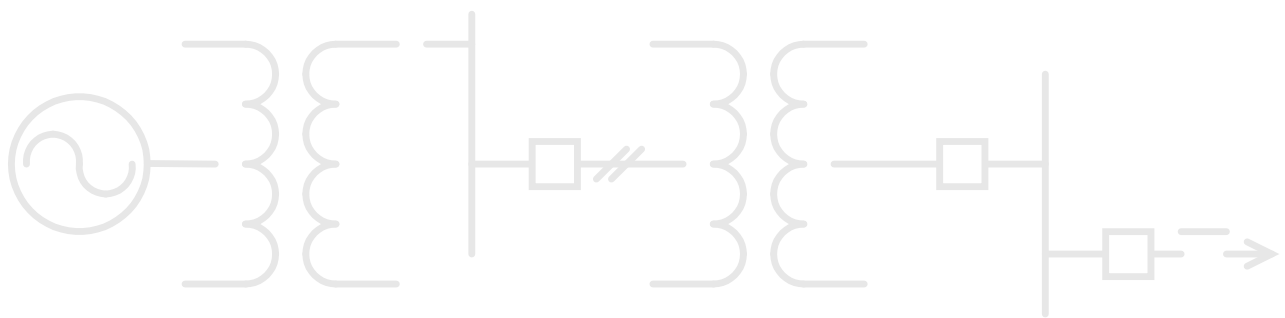
Integration of G500 with OpenVPN Client

Installation and Configuration Guide

SWM0103

Version 1.00 Revision 0

Associated Software Release: Version 1.00



COPYRIGHT NOTICE

© 2019, General Electric Company. All rights reserved.


The Software Product described in this documentation may only be used in accordance with the applicable License Agreement. The Software Product and Associated Material are deemed to be “commercial computer software” and “commercial computer software documentation,” respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable, and are delivered with Restricted Rights. Such restricted rights are those identified in the License Agreement, and as set forth in the “Restricted Rights Notice” contained in paragraph (g) (3) (Alternate III) of FAR 52.227-14, Rights in Data-General, including Alternate III (June 1987).

If applicable, any use, modification, reproduction release, performance, display or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the “Documents”) subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company. If applicable, any use, modification, reproduction, release, performance, display, or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

TRADEMARK NOTICES

GE and  are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company.

Serial/IP is a registered trademark of Tactical Software, LLC.

Tactical Software is a registered trademark of Tactical Software, LLC.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

Contents

About this Document	7
Purpose of this Document.....	7
Intended Audience.....	7
Additional Documentation	7
Safety words and definitions.....	8
Product Support	9
GE Grid Solutions Web Site.....	9
GE Technical Support Library.....	9
Contact Technical Support.....	9
1. Overview	10
1.1 Supported Client Devices.....	10
1.2 Setup Procedure.....	10
2. Setting up a Certification Authority	12
2.1 Setting up the XCA Certification Authority	12
3. Server & Client Certificate Generation	16
3.1 Generating Certificates Using XCA	16
4. Installing Certificates	23
4.1 Installing CA Certificate, Server Certificate and Diffie Hellman Parameters on the G500 23	23
4.2 Installing Client Certificate in Windows Server 2012 R2	25
4.3 Installing Client Certificate in Windows 7 PC.....	27
4.4 Installing Chain of CA Certificates on the G500.....	32
5. Configuring VPN Server in G500	35
5.1 Configuring VPN Server.....	35
5.2 VPN Server Log	40
6. Exporting VPN Client Configuration	41
7. Configuring OpenVPN Client	43
8. Revoking a Client certificate	47
8.1 Revoking the Certificate in XCA.....	47
8.2 Exporting the CRL in XCA.....	47

8.3	Installing the CRL in the G500	48
9.	Running OpenVPN Client as Windows Service using NSSM	49
9.1	How to install NSSM.....	49
9.2	How to Use NSSM.....	49
9.3	Running OpenVPN as Windows Service Using NSSM	50
9.4	Setting Up OpenVPN as a Service	50
A.	Certificate Error Messages Logged by OpenVPN Configuration HMI	56
B.	OpenVPN Server Log Messages.....	60
C.	VPN Client from Ubuntu PC.....	62
D.	List of Acronyms	63

Figures

Figure 1: G500 OpenVPN Configuration & Installation Flow Diagram..... 11

Tables

Table 1	Example Distinguished Name Components	13
Table 2	Example Distinguished Name Components	17
Table 3	Example Distinguished Name Components	19
Table 4	Location of Files Exported by Certification Authorities	23
Table 5	VPN Server Configuration Parameters	36
Table 6	Routing List and white Filter List	39
Table 7	ICMP White List Options	39
Table 8	List of Acronyms	63

About this Document

Purpose of this Document

This document describes how to establish a VPN (Virtual Private Network) channel between a G500 and an OpenVPN client running on a remote computer running Windows® Server 2012 R2 or Windows 7 for accessing one or more protected services in the substation. This document provides the procedures to:

- Implement a simple Certification Authority using XCA Certification Authority (Open-Source tool).
- Install certificates on the G500 and a Windows® Server 2012 running with OpenVPN client software.
- Configure OpenVPN server in G500 to communicate to OpenVPN client.
- Configure OpenVPN client to communicate to the G500 over virtual private network.

Intended Audience

This document serves as a reference for utility personal and systems integrators who wish to setup a VPN (Virtual Private Network) channel between a client device (Windows® Server 2012 R2 or Windows 7) and a G500 for the purposes of accessing one ore more protected services in the substation.

Additional Documentation





For further information about the Integration of G500 with OpenVPN Client, refer to the following documents:

- G500 Substation Gateway Software Configuration Guide, SWM0101
- G500 Substation Gateway, HMI Online Help

Safety words and definitions

Before attempting to install or use the device, review all safety indicators in this document to help prevent injury, equipment damage or downtime.

The following safety and equipment symbols are used in this document:

-  **DANGER** Indicates a hazardous situation which, if not avoided, will result in death or serious injury.
-  **WARNING** Indicates a hazardous situation which, if not avoided, could result in death or serious injury.
-  **CAUTION** Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.
-  **NOTICE** Indicates practices that are not related to personal injury.

Product Support

If you need help with any aspect of your GE Grid Solutions product, you can:

- Access the GE Grid Solutions Web site
- Search the GE Technical Support library
- Contact Technical Support

GE Grid Solutions Web Site

The GE Grid Solutions Web site provides fast access to technical information, such as manuals, release notes and knowledge base topics.

Visit us on the Web at: <http://www.gegridsolutions.com>

GE Technical Support Library

This site serves as a document repository for post-sales requests. To get access to the Technical Support Web site, go to: http://sc.ge.com/*SASTechSupport

Contact Technical Support

GE Grid Solutions Technical Support is open 24 hours a day, seven days a week for you to talk directly to a GE representative.

In the U.S. and Canada, call toll-free: 1 800 547 8629.

International customers call: +1 905 927 7070

Or send an e-mail to: multilin.tech@ge.com

1. Overview

A VPN (Virtual Private Network) channel is available between the G500 and an OpenVPN client running on a remote computer running Windows® Server 2012 R2 or Windows 7; this VPN channel allows access to one or more protected services in the substation. The VPN channel is implemented using OpenVPN, which uses a custom protocol based on TLS (Transport Layer Security), and certificate-based mutual authentication.

Certificates are issued by a Certification Authority (CA). Since the G500 is not delivered with a CA, you must make use of an existing CA or create your own. There are many third-party commercial and open-source CAs available. This document describes one open-source CA package:

- X Certificate and Key Management (XCA).

1.1 Supported Client Devices

This document describes how to install and configure the OpenVPN client in the following Devices.

- Windows® Server 2012 R2
- Windows 7

NOTICE

This document refers to installation of OpenVPN Client in Windows Server 2012 R2 and Windows 7, but the procedure should be similar for other Windows Operating Systems.

1.2 Setup Procedure

To establish a secure channel between an OpenVPN client and the G500:

1. Set up your CA; see section 2.1.2 .
2. Generate Diffie Hellman (DH) parameters; see Chapter 2.
3. Generate private key and certificate for your G500; see section 3.1.1 .
4. Generate client certificate + private key in .pk12 format for OpenVPN client running in Windows® Server 2012 R2 and Windows 7 PC; see section 3.1.2 .
5. Install the CA's Certificate on your G500; see section 4.1.
6. Install the private keys, certificates and Diffie Hellman parameters on your G500; see section 4.1.
7. Install .pk12 client certificate + private key into client device (Windows® Server 2012 R2 and Windows 7 PC) -see section 4.2.
8. Using the G500 HMI, configure the parameters for the OpenVPN Server; see section 5.1.
9. Using the "Export VPN Client File" option in the Utilities tab under Settings option, export the OpenVPN client configuration (*.ovpn) into a desired location; see section 5.2.
Note: Export VPN Client File Option is available in Utilities Tab under Settings option from Local HMI or from the Connected Mode in DS Agile MCP Studio only.
10. Securely copy the OpenVPN client configuration into the client device (Windows® Server 2012 R2 and Windows 7 PC).
11. Run the OpenVPN client software as a service or as a process in the client device (Windows® Server 2012 R2 and Windows 7 PC).
12. Test access to the protected service or device through the G500 OpenVPN server.

Figure 1 shows the sequence of steps involved in setting up an OpenVPN connection between a G500 and OpenVPN Clients.

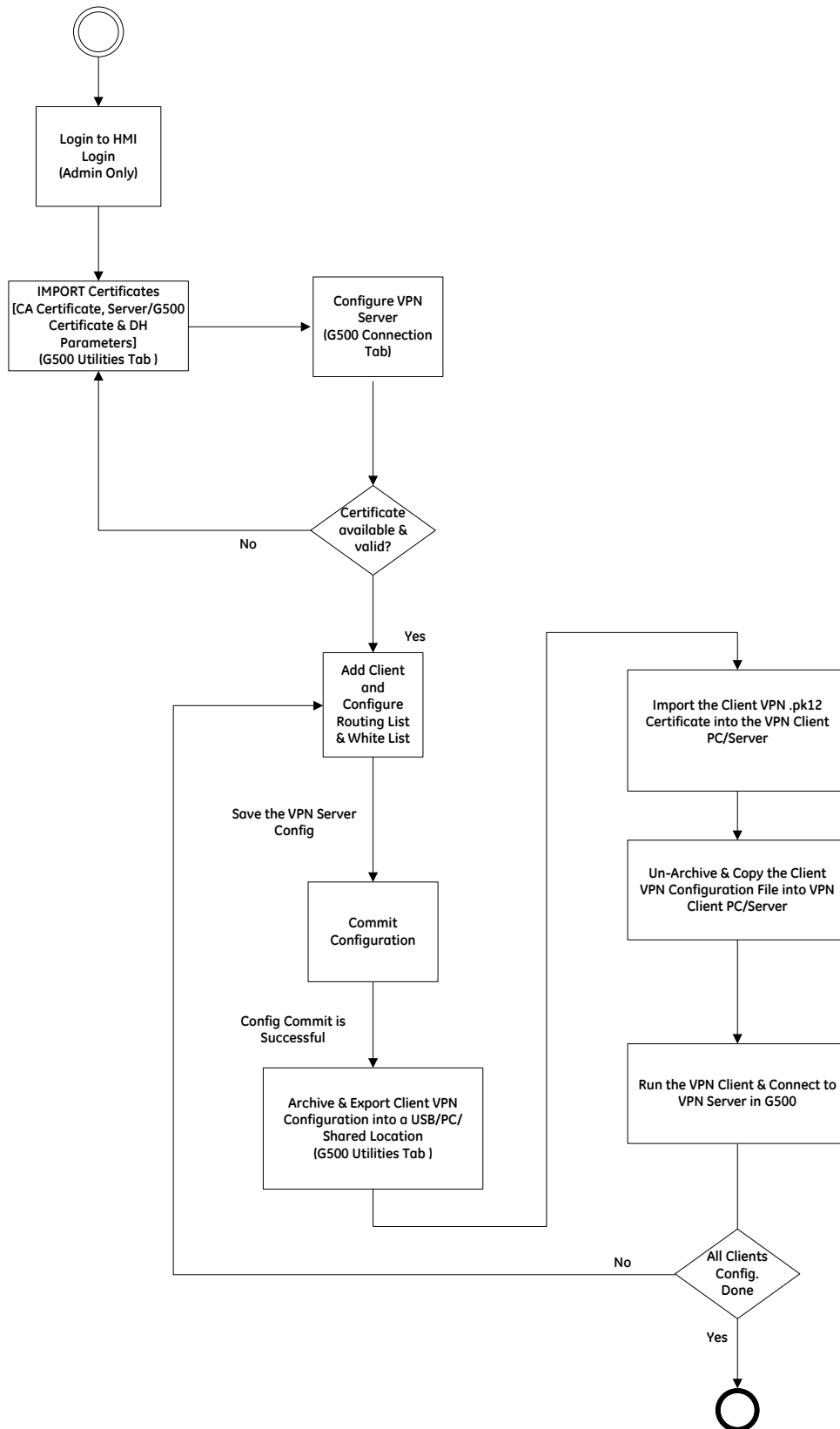


Figure 1: G500 OpenVPN Configuration & Installation Flow Diagram

2. Setting up a Certification Authority

Before you can configure a VPN connection between a client device and the G500 you need a Certification Authority (CA). In case you do not already have a CA, this chapter describes how to set up the XCA certification authority.

Once your CA is up and running, export the CA certificate so that you can install it on the client devices and the G500.

NOTICE

A CA that is planned for field use should be protected with strong security measures. Such measures include dedicating a computer for the CA, physically securing the computer, ensuring the computer is accessible only by authorized users, and not connecting the computer to a network. Such measures are required because a security breach of a CA would impact all devices that used certificates generated by the CA.

2.1 Setting up the XCA Certification Authority

XCA runs on Linux or Microsoft Windows. Below procedure explains the setting up of XCA Certification Authority for Windows.

The tasks performed to setup and initialize an XCA certification authority are:

1. Install XCA; see section 2.1.1
2. Create a database and initialize the CA; see section 2.1.2 .
3. Generate Diffie Hellman (DH) Parameters; see section 2.1.3 .

2.1.1 Install XCA

1. Download the latest version of XCA from: <http://sourceforge.net/projects/xca>.
2. Run the installation wizard to install XCA.

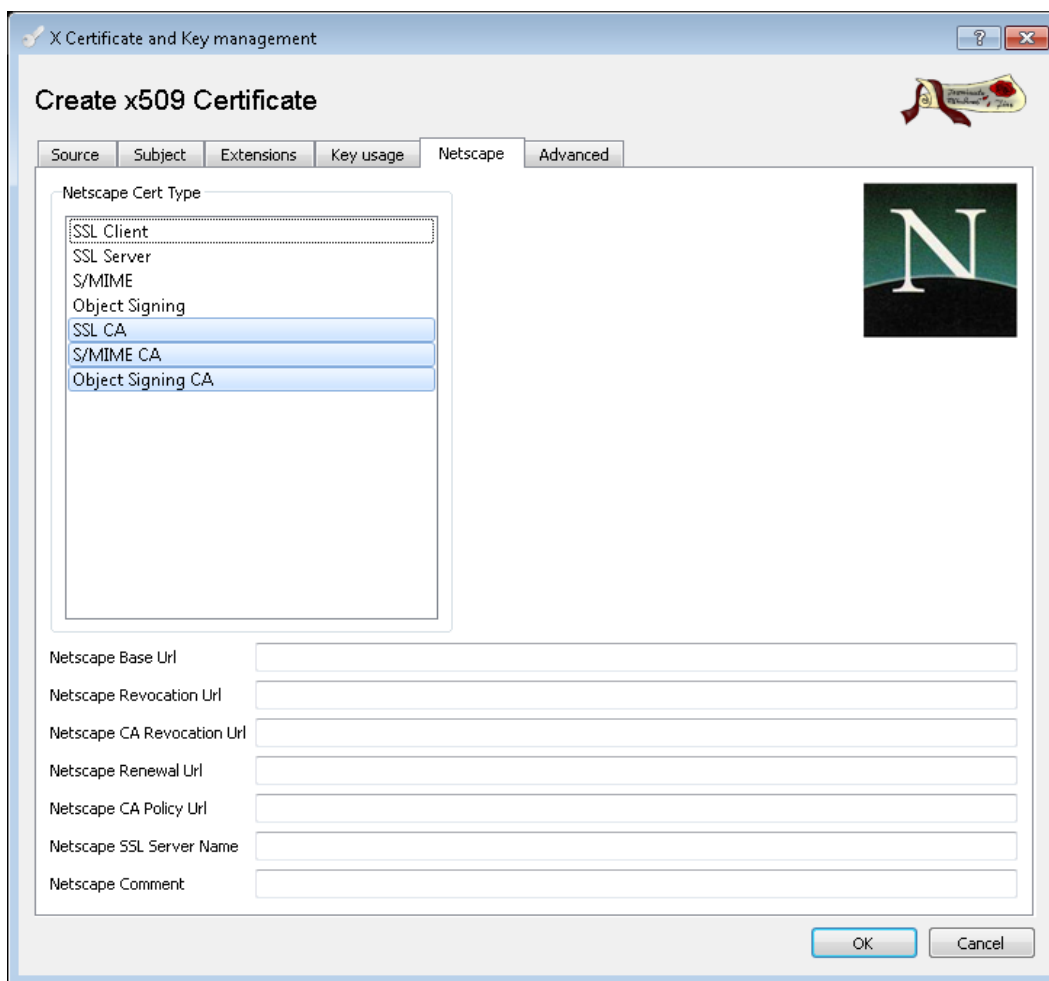
2.1.2 Create a Database and Initialize the CA

1. From XCA, select **File > New Database**.
2. Choose a protected location to save the database and then type in a strong password to encrypt the database.
3. Under the **Certificates** tab, choose **New Certificate**.
4. Under the **Source** tab, select the checkbox next to the label **Create a self signed certificate with the serial**. Change the dropdown named **Signature Algorithm** to "SHA 256" and leave the dropdown named **Template for the new certificate** as "[default] CA".
5. Under the **Source** tab, click **Apply All**.
6. Under the **Subject** tab, click the **Generate a new key** button.
7. In the dialog that appears, type in the name of the CA (e.g., "MyCA") in the **Name** field. Choose the **Keytype** as RSA. Change the **Keysize** to 2048.
8. Under the **Subject** tab, type in the distinguished name of the CA certificate. Table 1 provides example distinguished name components.

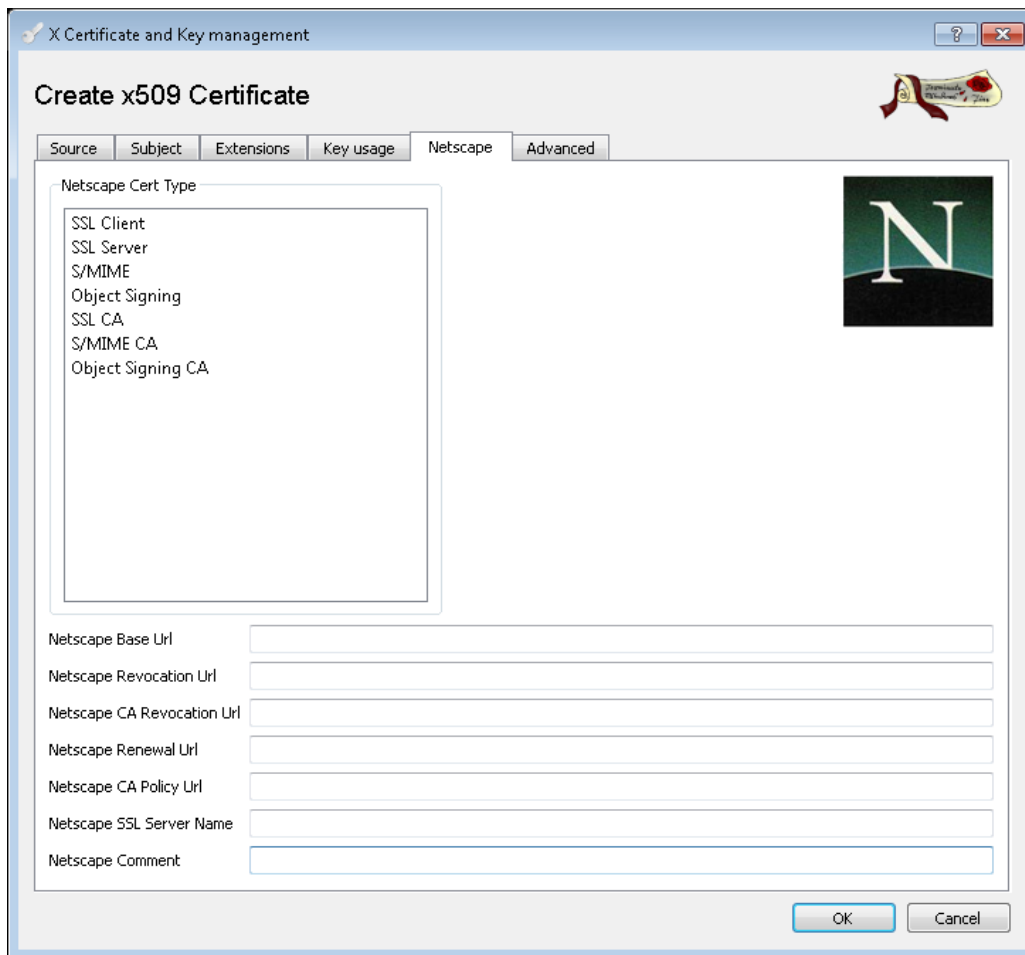
Table 1 Example Distinguished Name Components

Distinguished Name Component	Example
Internal name	MyCA
countryName	US
stateOrProvinceName	MyState
localityName	MyCity
organizationName	MyCompany
organizationalUnitName	MyDivision
commonName	MyCA
emailAddress	mail@my.domain

9. Under the **Extensions** tab, if necessary change the **Time Range** that the CA certificate is valid for and click **Apply**. The default is 10 years. Certificates generated with this CA certificate after this period are no longer valid.
10. Under the **Key usage** tab, do not change the defaults.
11. Under the **Netscape** tab, remove the value in the **Netscape Comment** field.



- Under the Netscape Cert Type, de-select **SSL CA, S/MIME CA, Object Signing CA** options.



Result: Under the **Advanced** tab, the following messages appear, except the value of the X509v3 Subject Key Identifier, which differs from key to key:



If above message does not appear, click **Validate** to view the message.

- Click **OK**.
Result: You now have a CA certificate to sign your G500 (Server) and Client certificates.
- Under the **Certificates** tab of the main view of XCA, select the new Certification Authority and click on **Export**.
- Ensure the **Export Format** is set to **PEM**.
- Browse to a protected directory (e.g., **My Documents > MyXCAFiles**) and click **Save**.
- Click **OK**.
Result: The file is named based upon the internal name of your CA with a .crt extension.

2.1.3 Generate Diffie Hellman (DH) Parameters

1. From XCA, select **Extra > Generate DH parameter**.
2. Enter a key size of 2048 and click **OK**.
Result: It may take a few minutes for the parameters to be generated and XCA may appear to be non-responsive. Be patient and allow XCA to complete.
3. When prompted, save the generated DH parameters file in a protected location (e.g., My Documents->MyXCAFiles) and leave the name as dh2048.pem.

3. Server & Client Certificate Generation

This chapter describes how to generate private keys and certificates for both the Client computer and the G500. These certificates allow the Client to authenticate itself to the G500 and the G500 to authenticate itself to the Client.

There are two types of certificates you can generate:

- The server certificate.
The server certificate identifies a G500.
- The client certificate in .pk12 format.
The client certificate identifies a particular user or a computer that is connected to the G500.

3.1 Generating Certificates Using XCA

3.1.1 Generating a G500 Server Certificate

A G500 Server certificate allows the G500 to authenticate itself to a Client. The G500 Server certificate contains a **commonName** field. This field should uniquely identify the G500 in your network.

To generate a G500 Server Certificate:

1. Launch XCA from the Windows Programs menu.
2. In the tree view of the **Certificates** tab, select the branch containing your Certification Authority.
3. Under the **Certificates** tab, click the **New Certificate** button.
4. Under the **Source** tab:
 - a. Select the checkbox next to the label **Use this Certificate for signing**. On the dropdown to the right of this checkbox, select the CA you created in section 2.1.2 (e.g., MyCA).
 - b. Change the dropdown **Signature Algorithm** to **SHA 256**.
 - c. Change the dropdown **Template for the new certificate** to “[default] HTTPS_server”.
 - d. Click **Apply all**.
5. Under the **Subject** tab, click the **Generate a new key** button.
6. In the dialog that appears, type in a name that uniquely identifies the G500 in your network (for this example, “MyG500”). Choose **Keytype** to RSA. Change the **Keysize** to 2048.
7. Click **OK**.
8. Go back to the **Subject** tab and type in the Distinguished name of the G500 server certificate. The most important component is the **commonName**. This is the name that your Clients is configured to accept. Any difference between the commonName of the certificate and the name configured in the Client results in a failed connection. Choose other name components that are appropriate for your company. Table 2 provides example distinguished name components.

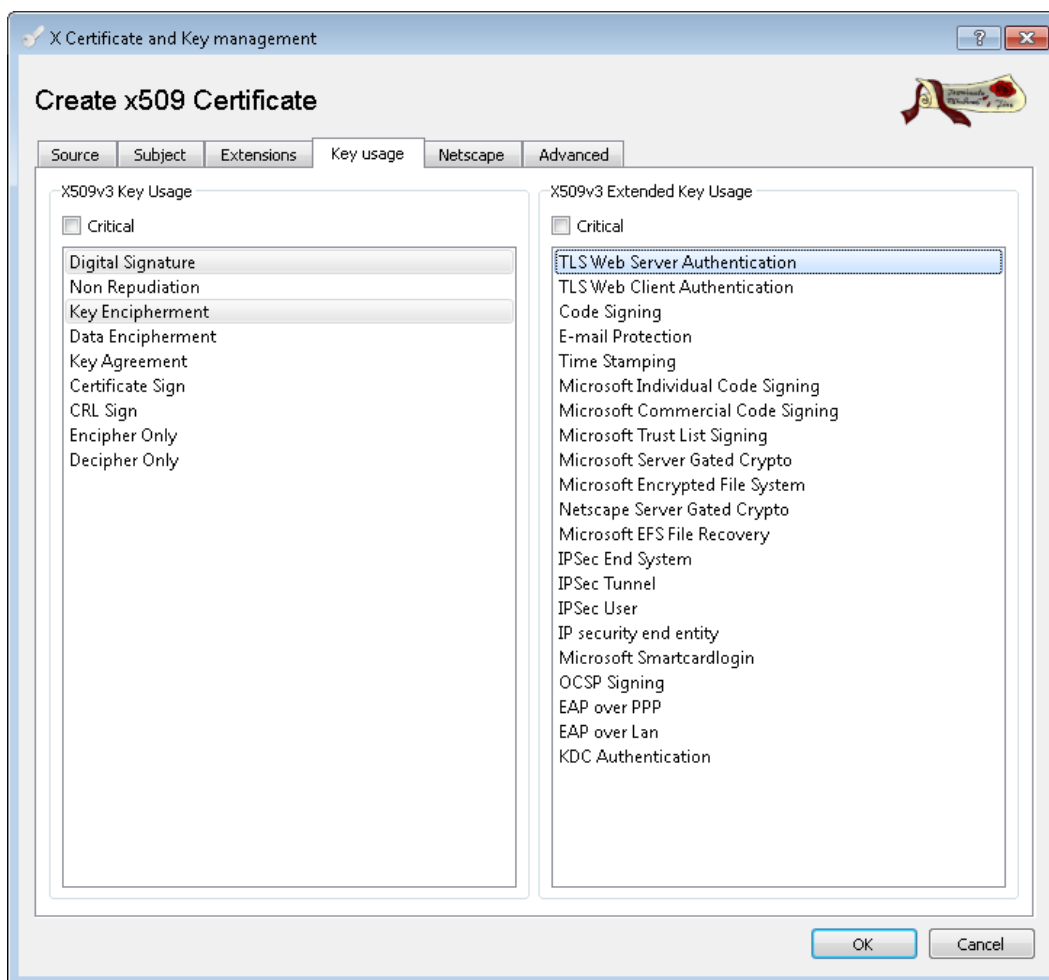
Table 2 Example Distinguished Name Components

Distinguished Name Component	Example
Internal name	MyG500
countryName	US
stateOrProvinceName	MyState
localityName	MyCity
organizationName	MyCompany
organizationalUnitName	MyDivision
commonName	MyG500
emailAddress	mail@my.domain

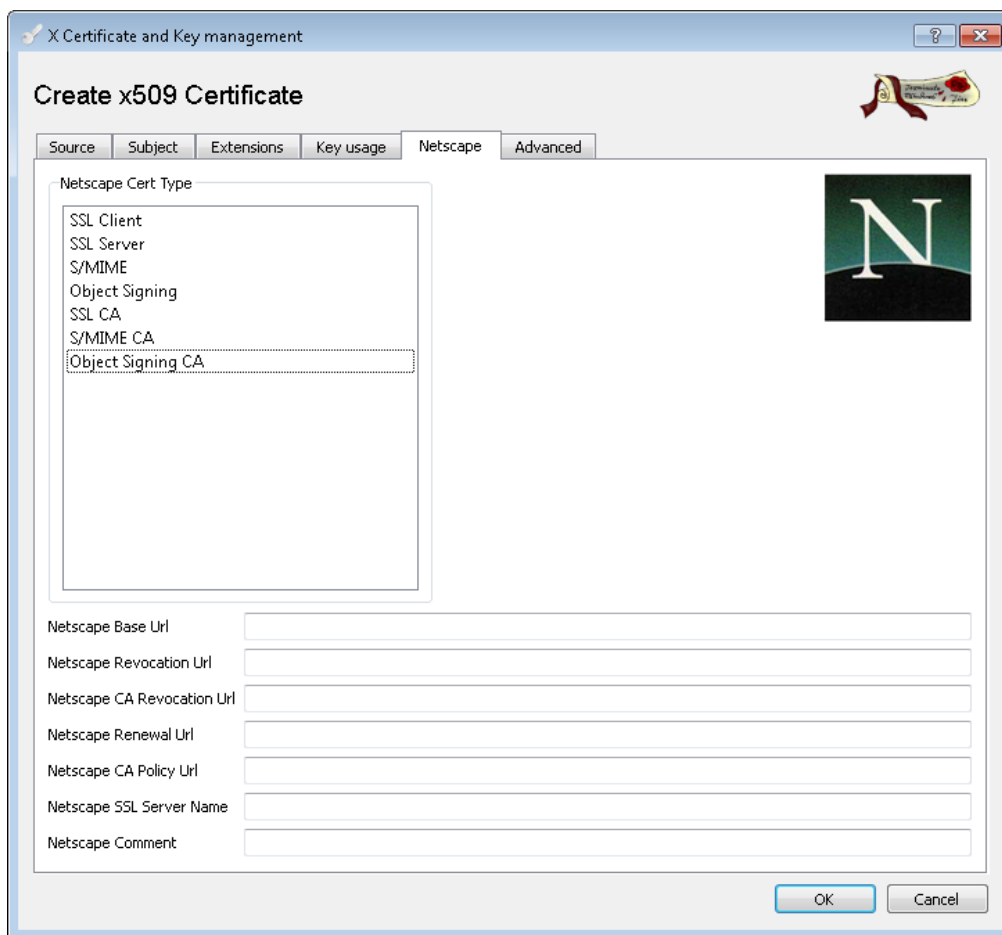
- Under the **Extensions** tab, if necessary change the **Time Range** that the CA certificate is valid for and click **Apply**. The default is one year.

The shorter the Time Range the more secure the certificate, but the more often you need to regenerate G500 Server certificates and deploy them into your G500s.

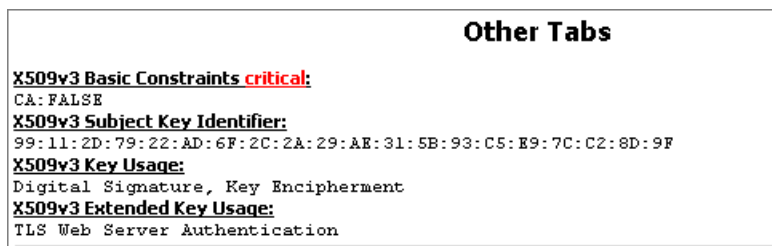
- Under the **Key usage** tab, under X509v3 Key Usage select **Digital Signature** and **Key Encipherment** and under X509v3 Extended Key Usage select **TLS Web Server Authentication** as shown below.



- Under the **Netscape** tab, remove the **Netscape comment** and under the **Netscape Cert Type**, if **SSL Server** is selected then deselect it from the list.



- Under the **Advanced** tab, click **Validate**. The following messages are expected except the value of the X509v3 Subject Key Identifier, which differs from key to key:



If above message is not displayed, click **Validate** to see the message.

- Click **OK**. You now have a G500 Server certificate.
- In the tree view under the **Certificates** tab, open the branch labeled according to your Certificate Authority, and select the new Server certificate.
- Click **Export**.
- In the dialog that appears, ensure the **Export Format** field is set to “PEM Cert + key”. Browse to a protected location (e.g., My Documents->MyXCAFiles) and click **Save**. Finally click **OK**. The certificate and private key will be in a file named with your G500’s Internal Name with the extension .pem (e.g., MyG500.pem).

NOTICE

This file is sensitive so keep it protected at all times. Delete all copies of the file after it has been installed on the G500. The file can be exported again from XCA if necessary.

3.1.2 Generating a Client Certificate

A Client certificate allows the Client to authenticate itself to a G500. The Client certificate contains a **commonName** field.

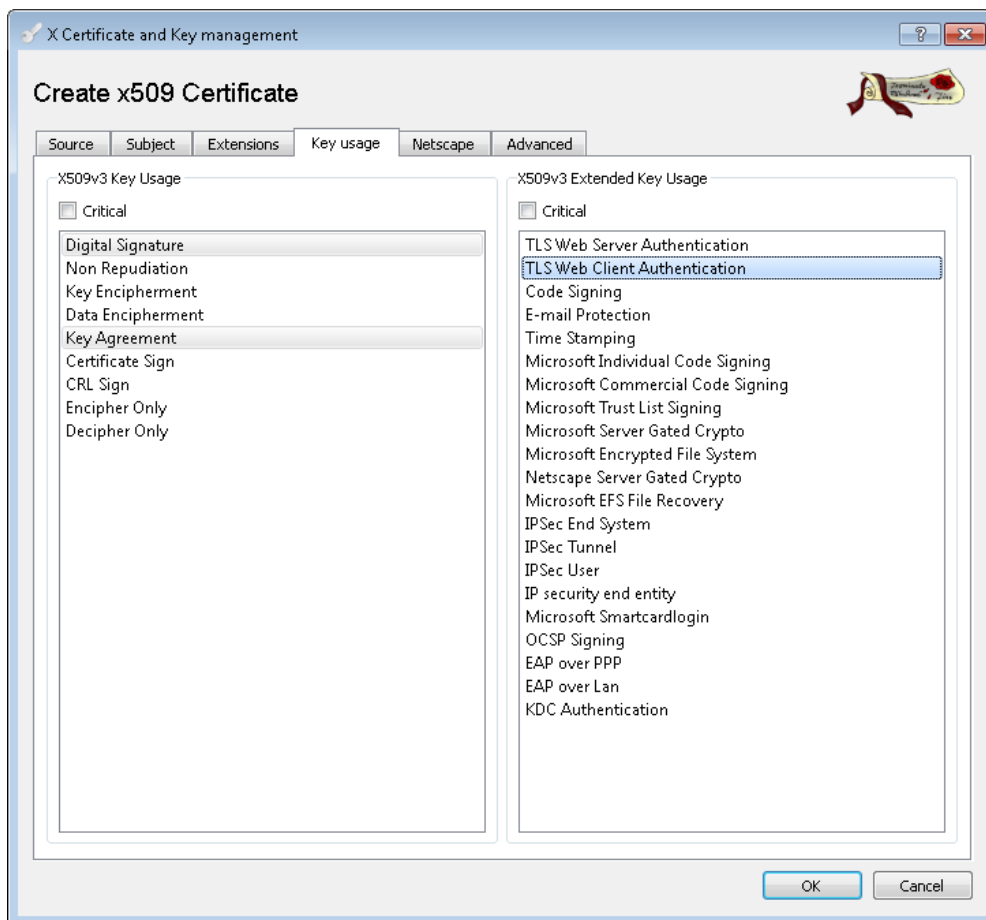
To generate a Client certificate:

1. Launch XCA from the Windows Programs menu.
2. In the tree view of the **Certificates** tab, select the branch containing your Certification Authority.
3. Under the **Certificates** tab, click the **New Certificate** button.
4. Under the **Source** tab,
 - a. Select **Use this Certificate for signing** checkbox. On the dropdown to the right of this checkbox, select the CA you created in section 2.1.2 (e.g., MyCA).
 - b. Change the dropdown **Signature Algorithm** to **SHA 256**.
 - c. Change the dropdown **Template for the new certificate** to "[default] HTTPS_client".
 - d. Click **Apply all**.
5. Under the **Subject** tab, click the **Generate a new key** button.
6. In the dialog that appears:
 - a. Type in a name that uniquely identifies the Client (for this example, that is **MyCA_client1**).
 - b. Choose **Keytype - RSA**.
 - c. Change the **Keysize** to 2048.
 - d. Click **OK**.
7. Go back to the **Subject** tab and type in the Distinguished name of the Client certificate. The most important component is the **commonName**. This is the name that the G500 is configured to accept. Any difference between the **commonName** of the Client certificate and the name configured in the G500 results in a failed connection.
8. Choose other name components that are appropriate for your company. Table 6 provides example distinguished name components.

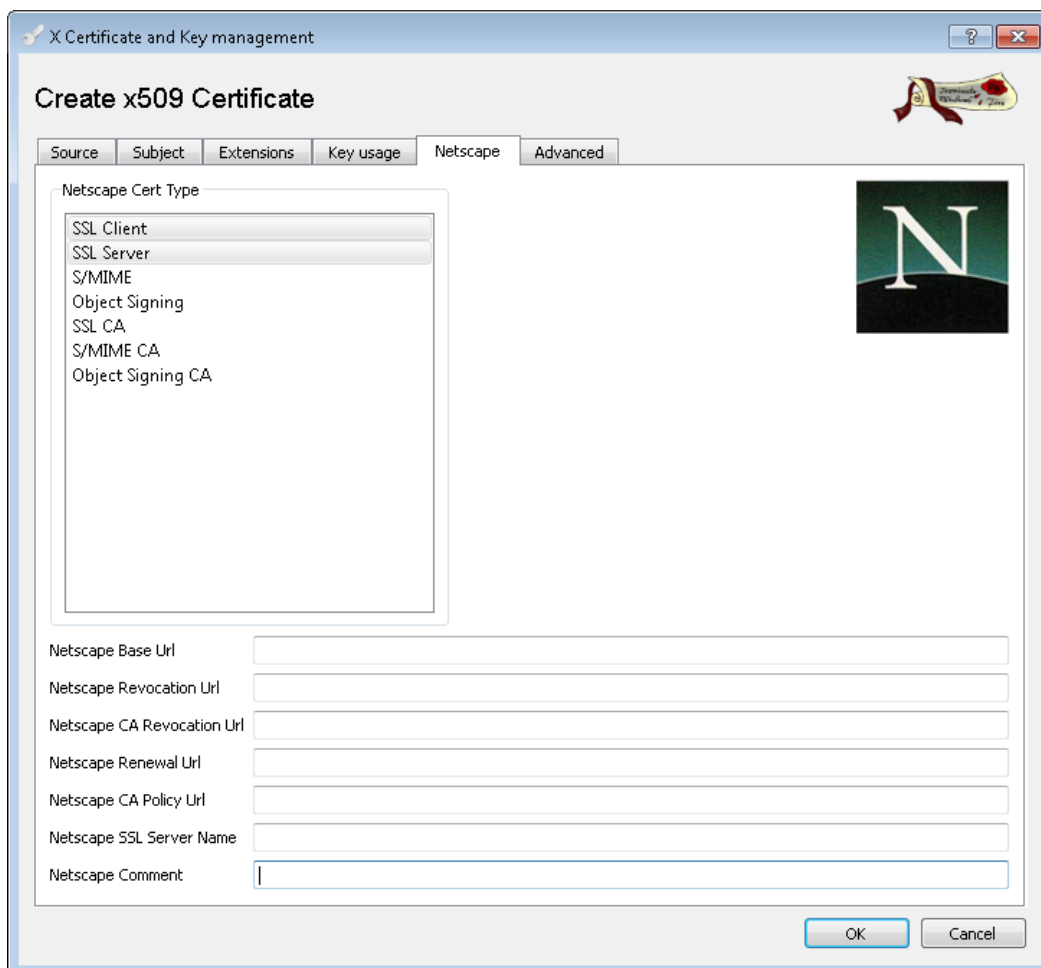
Table 3 Example Distinguished Name Components

Distinguished Name Component	Example
Internal name	MyCA_client1
countryName	US
stateOrProvinceName	MyState
localityName	MyCity
organizationName	MyCompany
organizationalUnitName	MyDivision
commonName	MyCA_client1
emailAddress	mail@my.domain

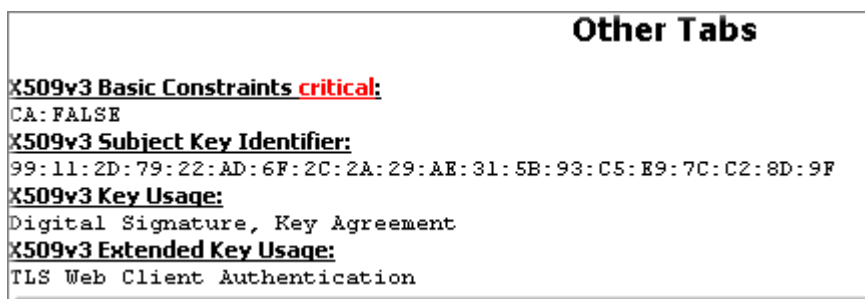
9. Under the **Extensions** tab, if necessary change the **Time Range** that the CA certificate is valid for and click **Apply**. The default is one year. The shorter the Time Range the more secure the certificate, but the more often you need to regenerate Client certificates and deploy them into Clients.
10. Under the **Key usage** tab, under X509v3 Key Usage select **Digital Signature** and **Key Agreement** and under X509v3 Extended Key Usage select **TLS Web Client Authentication** as shown below.



- Under the **Netscape** tab, remove the **Netscape comment** and under the **Netscape Cert Type**. And, if **SSL Client** and **S/MIME** is selected then deselect them from the list.



- Under the **Advanced** tab, click **Validate**. The following messages are expected except the value of the X509v3 Subject Key Identifier, which differs from key to key:



If above message does not appear, click **Validate** to view the message.

- Click **OK**.
Result: You now have a Client certificate.
- In the tree view of the **Certificates** tab, open the branch labeled with your Certification Authority and select the new Client certificate.
- Click **Export**.

16. In the dialog that appears, ensure the **Export Format** field is set to "PKCS #12(*. p12)". Browse to a protected location (**e.g., My Documents->MyXCAFiles**) and click **Save**. Finally click **OK**. **A Password dialog will be prompted to enter the Password to encrypt the PKCS#12 file**. The client certificate and its private key are encrypted and stored in a file named with the Internal Name of your client certificate and the(*.p12) extension (e.g., MyName.p12).
17. The same password will need to be used to import "*. p12" file in the Windows Server/Windows PC in which VPN Client will be running.

NOTICE

This file is sensitive so keep it protected at all times. Delete all copies of the file after it has been installed on the client.

4. Installing Certificates

This chapter describes how the CA Certificate, Server Certificate, Client Certificates and DH Parameters are installed. Table 4 summarizes where to get the files containing the CA certificate, Server certificates, Client Certificates and DH parameters.

Table 4 Location of Files Exported by Certification Authorities

Files	Location
CA Certificate	The CA certificate is in a file downloaded to a location of your choice as described in Section 2.1.2 . The file is named with a .crt extension (e.g., MyCA.crt).
Server Certificate and Key	Server certificate and key are in the same file under the location of your choice as described in Section 3.1.1 . The file is named with a .pem extension (e.g., MyG500.pem).
DH Parameters	DH parameters are in the file named dh2048.pem under the location of your choice as described in Section 2.1.3 .

4.1 Installing CA Certificate, Server Certificate and Diffie Hellman Parameters on the G500

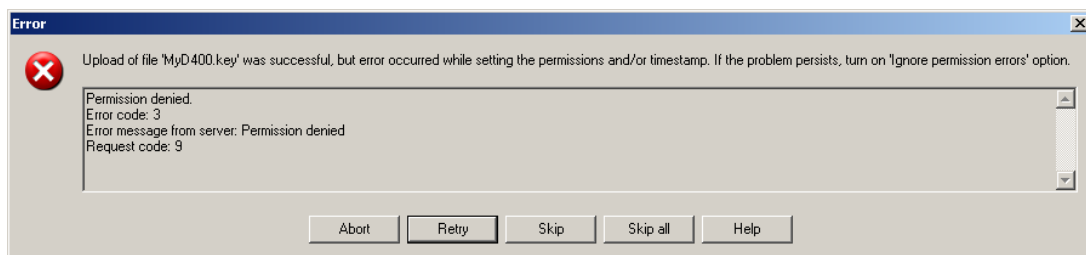
- Referring to Table 4 for file names and locations, copy the files containing the CA certificate, Server certificate, and DH parameters to one of two locations:
 - The folder /mnt/usr/SecureScadaTransfer on the G500. In this case, use an SFTP/SCP file transfer program such as WinSCP or Secure File Browser from DS Agile MCP Studio(Refer to Appendix B in SWM0101 for details).
 - The directory \SecureScadaTransfer on a USB drive.

Note: Do not install client certificates on the G500.

NOTICE

These files are sensitive, so keep them protected at all times. Delete these files from the USB drive after they have been installed on the G500.

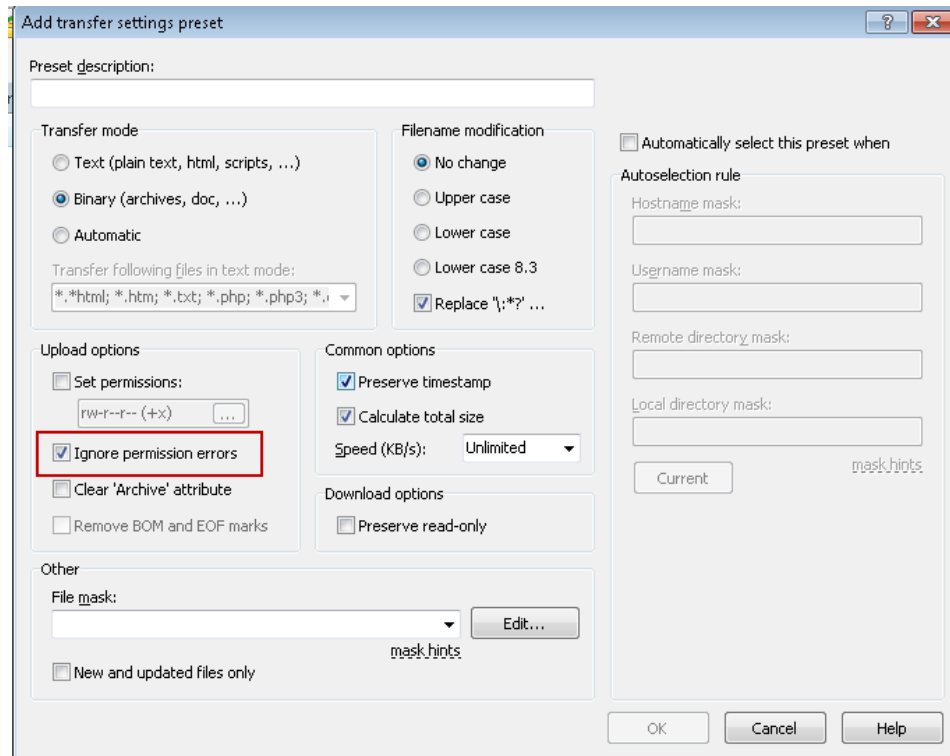
- If you are using WinSCP or Secure File Browser from DS Agile MCP Studio (Refer to Appendix B in SWM0101 for details) to transfer the files, you may get the following warning message:



The reason for this warning is that the G500 file system does not support per-file permissions, so when WinSCP or Secure File Browser from DS Agile MCP Studio(Refer to Appendix B in SWM0101 for details) tries to set the permissions on a file, it is unable to do so. However,

there is no security risk because the file takes on the default permissions of the files system which are correct. Therefore, this warning can be safely ignored by clicking **Skip**.

- To prevent this warning from appearing in the future, in WinSCP or Secure File Browser from DS Agile MCP Studio (Refer to Appendix B in SWM0101 for details) go to **Options > Preferences**. Then select **Transfer** and click **Ignore permission errors**.



- If you are using the USB drive method of transferring the files, insert the drive into any USB slot on the G500.
- Connect to the G500 with a browser and click the Utilities tab under Settings option from the power bar.

Note: This Option is available in Utilities Tab under Settings option from Local HMI or from the Connected Mode in DS Agile MCP Studio only.

- Click the **Import** button.
Result: A dialog box appears indicating that 1 Local Certificate and 1 Issuer Certificate was successfully imported. Click **OK** to dismiss the dialog.
- Click the **Manage** button, and then click the **Local** tab.
Result: A dialog box appears showing the Local certificate details in the Staged Local Certificates area.
- Select the certificate and click **Install**.
Result: The certificate moves into the Installed Local Certificate area. This also installs the DH parameters file.
- Click the **Issuer** tab.
Result: The CA certificate appears in the Staged Issuer Certificates area.
- Select the row containing the CA certificate and click **Install**.
Result: The certificate moves into the Installed Issuer Certificates area.

11. Close the dialog and log out of the G500.

Note: If the G500 is part of a redundant system, follow the below steps.

1. Switchover to the Standby G500.
2. Repeat steps 1 to 11.
3. Switchover back to the Original G500.
4. Ensure the standby configuration is in sync with the active configuration (i.e., Standby Config Out of Sync DI = Config In Sync)
5. Reboot the standby G500.

4.2 Installing Client Certificate in Windows Server 2012 R2

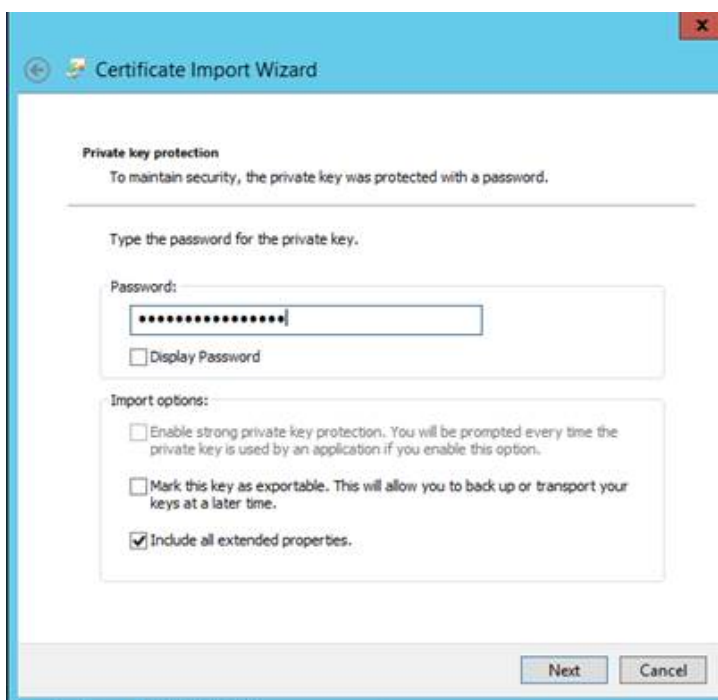
To import the "*.p12" file (encrypted PKCS#12 file that has Client Certificate + Private Key) into the Local Machine Store or Current User of Windows 2012 Server:

1. Securely Copy the "*.p12" (e.g., MyName.p12) file to the Windows 2012 R2 Server where VPN client will run.
2. Right-click on the "*.p12" file and select option: **Open with -> Crypto Shell Extensions**.
3. If you are running OpenVPN as a service, select **Local Machine**. Otherwise, select **Current User**.



4. Click **Next > Next**.
5. Enter the same password that was used to encrypt the "*.p12" file as part of Client Certificate + Private Key creation using XCA tool (Refer to Section 3.1.2).
6. It is recommended that you do not select **Mark this key as exportable** as shown below.

7. Select option **Include all extended properties** as shown below.
8. If you are running OpenVPN as a service, the option **Enable strong private key protection** is not available as shown below. If you are running OpenVPN as a user, select option **Enable strong private key protection** for added protection.



9. Click **Next**.
10. Select option: **Automatically select the certificate store based on the type of certificate**.



11. Click **Next**
Result: An operation summary appears.



12. Click **Finish**.

Result: A message appears, indicating that the import was successful.

13. Click **OK**.

Result: The client certificate should now be in the local machine store.

NOTICE

Delete the "*. p12" file on the file system because it is sensitive and no longer required to be on the file system.

4.3 Installing Client Certificate in Windows 7 PC

To import the "*. p12" file (encrypted PKCS#12 file that has Client Certificate + Private Key) into a Windows 7 PC:

1. Securely Copy the "*. p12" (e.g., MyName.p12) file using SCP/SFTP or USB into Windows 7 PC where VPN client will run.

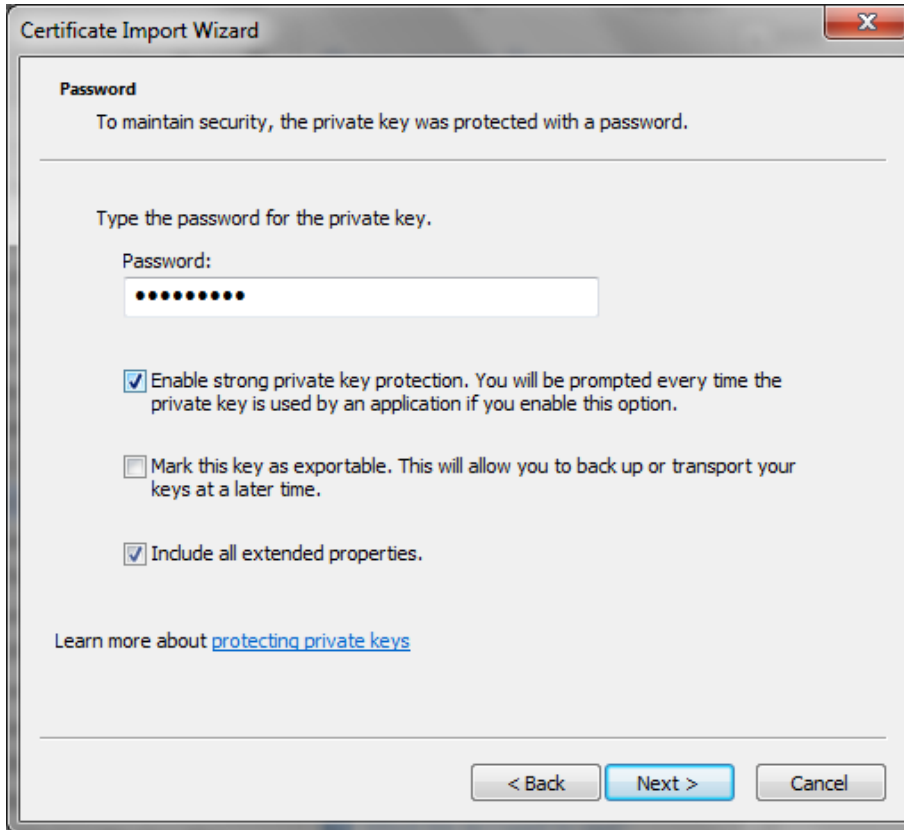
2. Double-click on the “*.p12” file.

Result: The Certificate Import Wizard window appears.



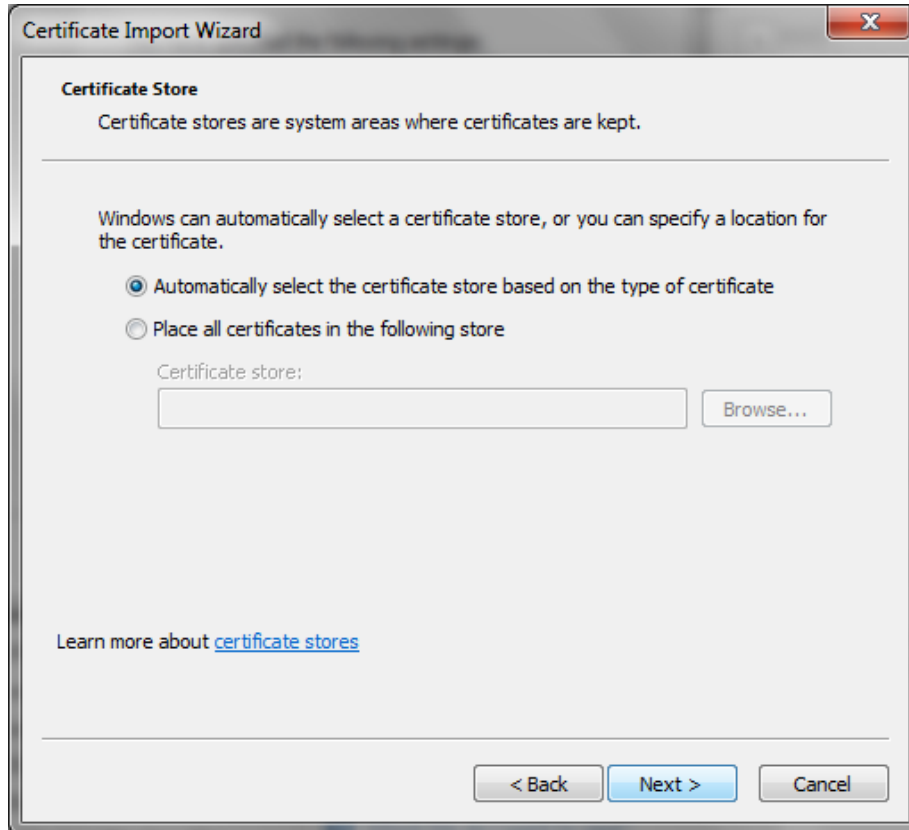
3. Click **Next > Next**.
4. Enter the same password that was used to encrypt the “*.p12” file as part of Client Certificate + Private Key creation using XCA tool (Refer to Section 3.1.2).
5. It is recommended that you do not select option: **Mark this key as exportable** as shown below.
6. Select option: **Include all extended properties**.

7. Select option: **Enable strong private key protection** for added protection.



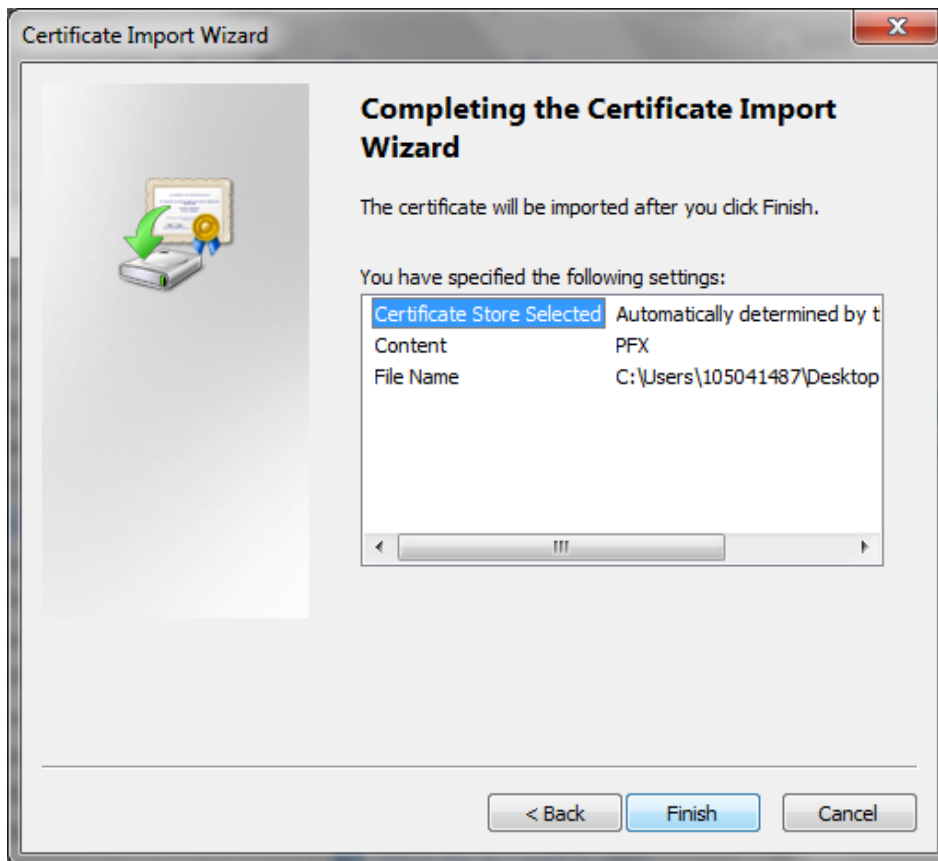
8. Click **Next**.

9. Select option: **Automatically select the certificate store based on the type of certificate.**



10. Click **Next**

Result: A summary of the operation appears.



11. Click **Finish**.

Result: The following window appears.



12. Click **OK**.

Result: A message appears, indicating that the import was successful.

13. Click **OK**.

Result: The client certificate should now be in the local machine store.

NOTICE

Delete the "*.p12" file on the file system because it is sensitive and no longer required to be on the file system.

4.4 Installing Chain of CA Certificates on the G500

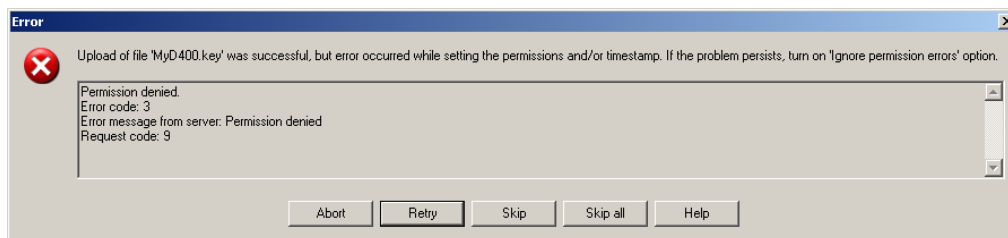
1. Referring to Table 4 for file names and locations, copy the files containing the CA certificate, Server certificate, and DH parameters to one of two locations:
 - The folder /mnt/user/SecureScadaTransfer on the G500. In this case, use an SFTP/SCP file transfer program such as WinSCP or Secure File Browser (Refer to Appendix B in SWM0101 for details).
 - The directory \SecureScadaTransfer on a USB drive.

Note: Do not install client certificates on the G500.

NOTICE

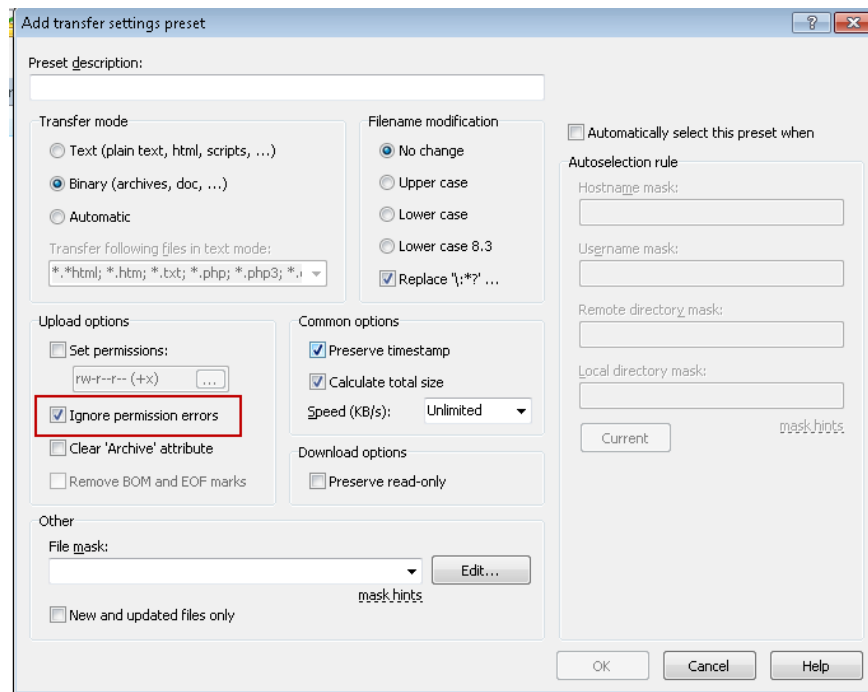
These files are sensitive, so keep them protected at all times. Delete these files from the USB drive after they have been installed on the G500.

2. If you are using WinSCP or Secure File Browser from DS Agile MCP Studio (Refer to Appendix B in SWM0101 for details) to transfer the files, the following warning message may appear:



The reason for this warning is that the G500 file system does not support per-file permissions, so when WinSCP or Secure File Browser from DS Agile MCP Studio (Refer to Appendix B in SWM0101 for details) tries to set the permissions on a file, it is unable to do so. However, there is no security risk because the file takes on the default permissions of the file system which are correct. Therefore, this warning can be safely ignored by clicking **Skip**.

- To prevent this warning from appearing in the future, in WinSCP go to **Options > Preferences**. Then select **Transfer** and click **Ignore permission errors**.



- If you are using WinSCP or Secure File Browser from DS Agile MCP Studio (Refer to Appendix B in SWM0101 for details) then copy all the CA certificates files in the chain, Server certificate, and DH parameters to folder `"/mnt/usr/SecureScadaTransfer"` on the G500.
- If you are using the USB drive method of transferring the files, insert the drive into any USB slot on the G500.
- Connect to the G500 with a browser and click the Utilities tab under Settings option from the power bar.

Note: This is available in Utilities Tab under Settings option from Local HMI or from the Connected Mode in DS Agile MCP Studio only.

- Click the **Import** button.
Result: A dialog box appears indicating that 1 Local Certificate and a list of all Issuer Certificates in the chain will be successfully imported. Click **OK** to dismiss the dialog.
- Click the **Manage** button, and then click the **Local** tab.
Result: A dialog box appears showing the Local certificate details in the Staged Local Certificates area.
- Select the certificate and click **Install**.
Result: The certificate moves into the Installed Local Certificate area. This also installs the DH parameters file.
- Click the **Issuer** tab.
Result: All the CA certificates in the chain appear in the Staged Issuer Certificates area.
- Select all the CA certificates in the chain and click **Install**.
Result: The certificates move into the Installed Issuer Certificates area.
- Close the dialog box and log out of the G500.

NOTICE

If a chain of certificates is being used, all the certificates in the chain must be installed.

Note:

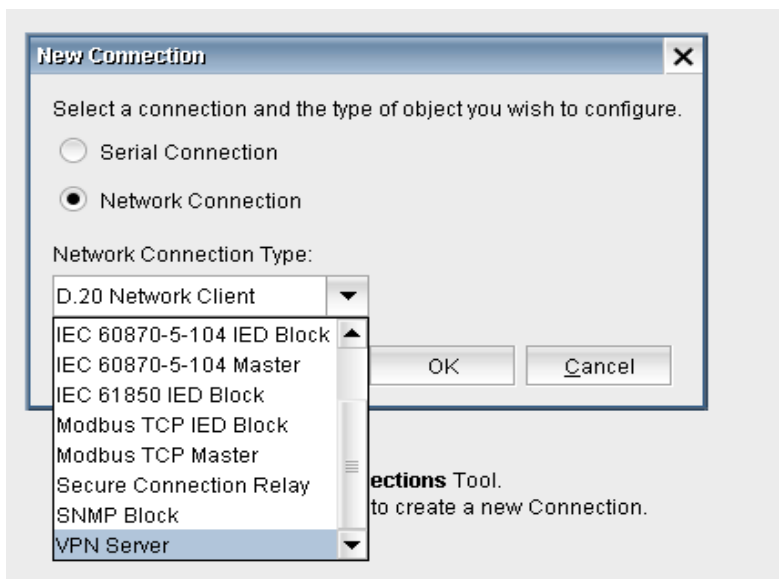
If the G500 is part of a redundant system:

1. Switchover to the Standby G500.
2. Repeat steps 1 to 12.
3. Switchover back to the Original G500.
4. Ensure the standby configuration is in sync with the active configuration (i.e. Standby Config Out of Sync DI = Config In Sync)
5. Reboot the standby G500.

5. Configuring VPN Server in G500

5.1 Configuring VPN Server

1. Login to G500 Online GUI as an Administrator user. Only users with administrator rights can configure and view OpenVPN configuration as shown below.
2. Go to Utilities tab under Settings option and install CA and Server Certificates – refer to Section 4.1
3. Go to the **Configuration** tab in DS Agile MCP Studio and then select **Network Connection** and Network Connection Type: **VPN Server**.



4. Configure the VPN Server settings as shown below.

Enter any additional options to add to the VPN Server Configuration here, separated by semicolon. EXAMPLE: renegotiate 900

Add/Remove Client Settings
The Client Name must match the Common Name of the client certificate

Name	Enabled	Routing List And White List
MyCA_client1	<input checked="" type="checkbox"/>	Configure
MyCA_client2	<input checked="" type="checkbox"/>	Configure
MyCA_client3	<input checked="" type="checkbox"/>	Configure
MyCA_client4	<input checked="" type="checkbox"/>	Configure
MyCA_client5	<input checked="" type="checkbox"/>	Configure
MyCA_client7	<input checked="" type="checkbox"/>	Configure
MyCA_client8	<input checked="" type="checkbox"/>	Configure
MyCA_client9	<input checked="" type="checkbox"/>	Configure

Note: Refer to Table 5 for a description of each setting in the VPN Server configuration.

Table 5 VPN Server Configuration Parameters

Setting	Description	Range	Default
Name	Unique name for the VPN Server.	Text string 32 characters are allowed	VPN Server
Auto Start	Indicates if the application automatically starts when the configuration is changed and reloaded or when the G500 re-boots.	Disabled Enabled	Enabled
Network IP Address	IP address of the device. Must be unique from other configured devices.	Valid IPv4 address and subnet mask. The supported subnet mask range is from 16 to 31 only.	10.200.0.0 /24
Port	The port number on which the device communicates.	0 to 65535	1,194
Concurrent Connections	The number of allowed concurrent connections.	1, 2, 3	1
Transport Layer	The transport layer protocol; either: <ul style="list-style-type: none"> Transmission Control Protocol (TCP), or User Datagram Protocol (UDP) 	TCP UDP	UDP

Setting	Description	Range	Default
Encryption Algorithm	Mathematical formula used in encryption and decryption of the VPN communication.	List of encryption algorithms. AES-256-CBC AES-256-CFB1 AES-256-CFB8 AES-256-OFB AES-192-CBC AES-192-CFB1 AES-192-CFB8 AES-192-OFB CAMELLIA-256-CBC CAMELLIA-256-CFB CAMELLIA-256-CFB1 CAMELLIA-256-CFB8 CAMELLIA-256-OFB CAMELLIA-192-CBC CAMELLIA-192-CFB CAMELLIA-192-CFB1 CAMELLIA-192-CFB8 CAMELLIA-192-OFB	AES-256-CBC
Authentication Algorithm	Authentication is the process of verifying the encrypted data was sent by the sender and was not altered.	List of authentication algorithms. SHA1-160 SHA-160 RSA-SHA1-160 RSA-SHA2-160 RSA-SHA-160 DSA-SHA1-160 DSA-SHA1-old-160 DSA-SHA-160 DSA-160 RIPEDMD160-160 RSA-RIPEDMD160-160 ecdsa-with-SHA1 SHA-224 RSA-SHA-224 SHA-256 RSA-SHA-256 SHA-384 RSA-SHA-384 SHA-512 RSA-SHA-512 whirlpool-512	SHA-256

Setting	Description	Range	Default
Custom Option	<p>Enter any options to be added to the VPN Server Configuration. All options appear in this field, separated by semicolons.</p> <p>To edit this field:</p> <ol style="list-style-type: none"> 1. Click the Edit button. Result: The Configure Custom Option window appears. 2. Click the Add button. Result: A line appears as a Custom Option. 3. Type in the option text. 4. Click Save. <p>NOTICE Custom Options are advanced options and take precedence over the standard configuration options. The standard options are secure by default. Implementing custom options can impact the security strength (e.g. using weak ciphers such as DES*, RC2-*, and BF-*). The customer assumes risk of weakened security when implementing custom options. Consult the online OpenVPN literature for guidance.</p>	<p>Text string</p> <p>For example:</p> <ul style="list-style-type: none"> • renegotiate-timeout 300 • tun-mtu 1500 ; mssfix 1300 • fragment 1400; • mssfix • tls-cipher TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA • socket-flags TCP_NODELAY • push "socket-flags TCP_NODELAY 	blank
Client Name	<p>The client common name.</p> <p>Note: This name must match the Common Name of the client certificate.</p>	<p>Text string</p> <p>32 characters are allowed</p>	Client1
Enabled	<p>Selected if the Client is enabled.</p> <p>Not selected if the Client is disabled</p>	<p>Enabled</p> <p>Disabled</p>	Enabled
Routing List and White List:	<p>Click Configure to access the Configure Routing List and the White List.</p>		

5. Configure Routing List and White List as shown in Table 6.

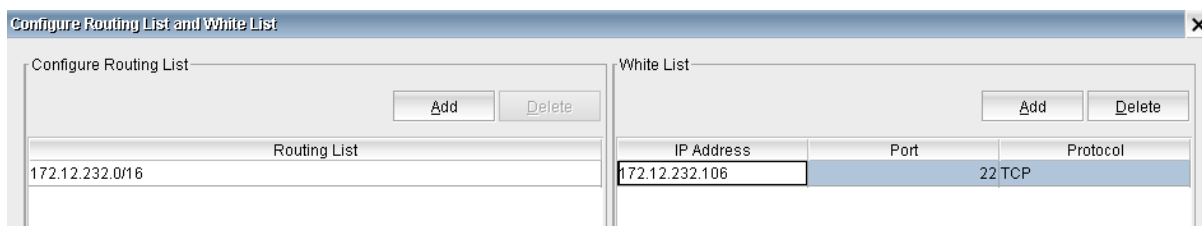
Table 6 Routing List and white Filter List

Setting	Description	Format	Example
Routing List	Drop down list of Route IP address & Subnet Mask in CIDR notation. Note: Routing List consist of list of configured networks (including VLANs & PRP) in G500. This list can't be edited by the User.	Valid IP4 Address/Netmask	172.12.232.0/16
White List	"IP/Port/Protocol Whitelist" for each VPN client to allow the incoming connections based on the combination of destination IP address, protocol and Port number through VPN tunnel.	IP Address: Valid IP4 Address Port No: Valid TCP/UDP Port Number Protocol: From the below drop-down list: <ul style="list-style-type: none"> • TCP • UDP • TCP+UDP • Any ICMP • Useful ICMP • Useful ICMP+ Ping ICMP Type/Code allowed combinations are described in Table 7 ICMP White List Options.	IP Address: 172.12.232.106 Port: 22 Protocol: TCP

Note: Port Number is available for TCP, UDP and TCP+UDP protocols only in White List configuration.

Table 7 ICMP White List Options

ICMP White List Option	Type	Code
Any ICMP	All	All
Useful ICMP and Useful ICMP + Ping	3 (Destination Unreachable)	All
	0 (Echo reply)	0
	11 (Time Exceeded)	0 (TTL expired in transit)
	11 (Time Exceeded)	1 (Fragment reassembly time expired)
Useful ICMP + Ping	8 (Echo request)	0



6. Save the VPN Server configuration and apply configuration commit to apply these changes.
Result: All VPN Server & Client configuration files are saved in the directory “/etc/openvpn/”.

Note: A static network route must be configured in each unique destination device referenced in all of the configured whitelists.

The route must be specified as follows:

Route Destination: The Network IP Address of the G500’s VPN Server Configuration.

Route Network Mask: The network mask of the Network IP Address of the G500’s VPN Server Configuration.

Route Gateway: The IP address of the G500 interface that is reachable by the destination device. In the case of G500 Redundant system, it would be Active IP address of the G500 interface that is reachable by the destination device.

5.2 VPN Server Log

G500 HMI provides support for VPN Server Log available to Administrator Users. This Log is available under System Logs button and can be used for diagnostic purposes.

This log is also available from the G500 command prompt for Administrator or Root Users and can be accessible using command:

sudo tail -f /var/log/G500 /openvpn.log

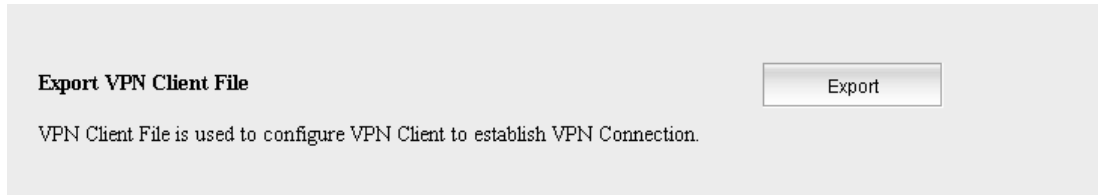
Refer to Appendix B for troubleshooting guide based on messages in this log.

6. Exporting VPN Client Configuration

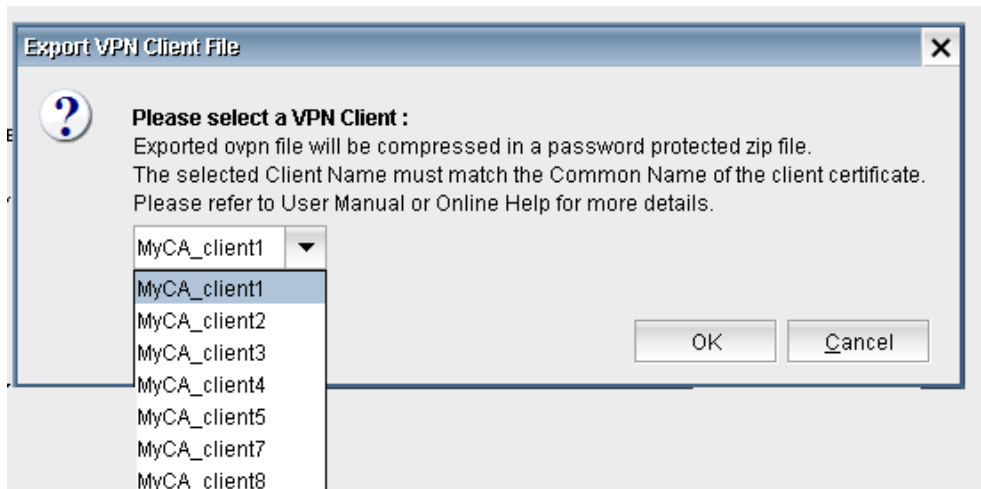
The VPN client configuration file is generated by G500. This client configuration is archived with password protection into a file and exported into a PC or a shared location using option Export VPN Client File from the Utilities tab under Settings options as described below.

To export a VPN Client file:

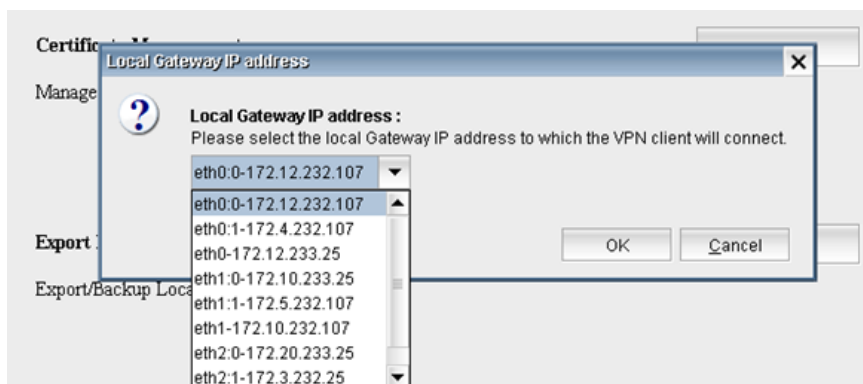
1. Go to Export VPN Client File option and click the **Export** button.



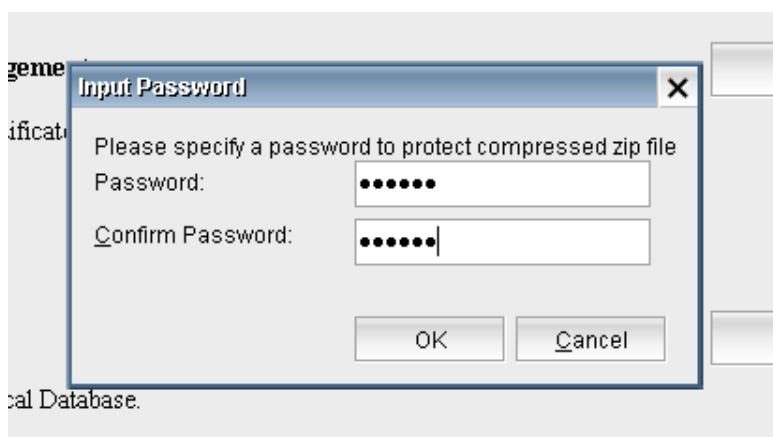
2. Select the Client from configured drop-down list of configured Clients.



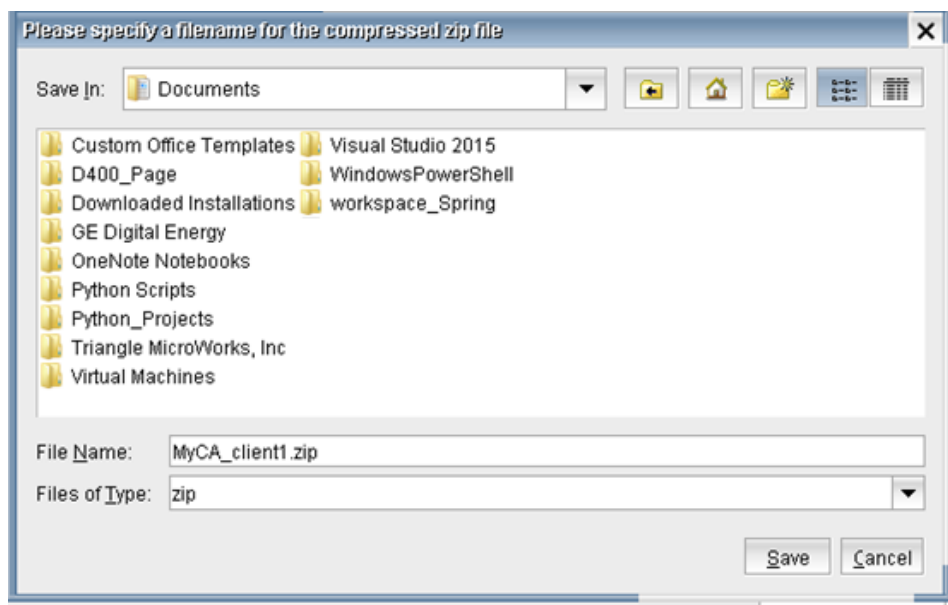
3. Select the Local Gateway IP address to which VPN Client will need to connect from the list of Configured IP address of G500.



4. Enter the Password to save the Client Configuration file in protected & compressed format. You need to use the same password to uncompress the Client configuration file using 7Zip or WinRAR software.



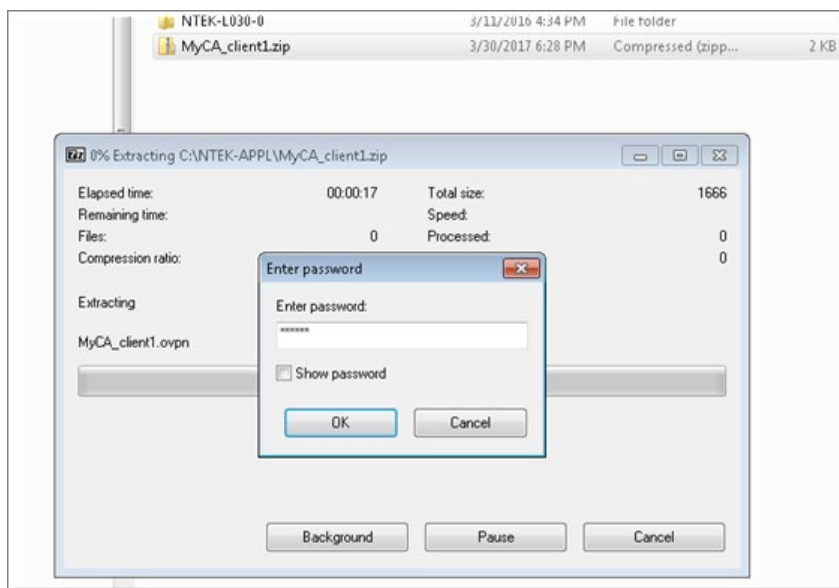
5. Securely save the file into a PC/Shared Location/USB.



Note: Exporting VPN Client Configuration options is also available through File Explorer functionality in Local HMI. The compressed Client Configuration file is available in the USB.

7. Configuring OpenVPN Client

1. Download OpenVPN Client software from the below link
<https://openvpn.net/index.php/open-source/downloads.html>
2. Install OpenVPN client software on Windows 7 PC or Windows 2012R2 Server.
3. After installation, the OpenVPN Client Configuration is present at the below folder.
C:\Program Files\OpenVPN\config.
4. Download 7zip or WINRAR software from the below links and install on Windows 7 PC or Windows 2012R2 Server.
www.7-zip.org/download.html
www.win-rar.com/download.html
5. Use either 7zip or WINRAR software uncompressing the password protected zip file generated in step 5 of Chapter 6. and copy the contents of the uncompressed file into this configuration folder:
C:\Program Files\OpenVPN\config\



NOTICE

It is important to install “.pk12” (Client Certificate + Private Key) before importing VPN Client Configuration into a Windows® Server 2012 or a Windows 7 PC.

6. You can start OpenVPN client as a Service on system startup in Windows 2012 R2 Server or Windows 7 PC as follows:
 - a. Run the Windows Service administrative tool:
 - b. Press **Windows Key + R**
 - c. Type **services.msc** and press **Enter**.
 - d. Find the OpenVPN service and set its Startup Type to "automatic."
 - e. Optionally, start the service now.

OR

If OpenVPN client could not start automatically on system startup in Windows 2012R2 Server or Windows 7 PC, then use NSSM (Non-Sucking Service Manager) Utility to start the OpenVPN client at system startup. Refer to Chapter 8.

7. OpenVPN client can run from GUI manually in Windows 2012R2 or Windows 7 PC. Refer to instructions in the below link to start OpenVPN Client from OpenVPN GUI.

<https://community.openvpn.net/openvpn/wiki/OpenVPN-GUI>

The contents of the Client VPN Configuration file for Windows® Server 2012 or Windows 7 PC appears similar to the example shown below:

```

# Automatically generated OpenVPN client config file
# Note: this config file contains inline private keys
#       and therefore should be kept confidential!
client
proto udp
remote 172.12.232.72
port 1194
nobind
dev tun
persist-key
persist-tun
keepalive 10 60
comp-lzo no
auth SHA1
cipher AES-256-CBC

<ca>
-----BEGIN CERTIFICATE-----
MIIC1DCCAbygAwIBAgIBATANBgkqhkiG9w0BAQUFADANMQswCQYDVQQDEwJDQTAE
Fw0xNzA0MjAyMTU0MDEBaFw0yNzA0MjAyMTU0MDEBaMA0xCzAJBgNVBAMTAkNBMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAc1FoIw1AvmFHlsaZAuOv65E
cpFLbQL3DhnE4/FOqSTPXSabBMu7IwtJPSPkBnmE8u4owttapLWoYE/D+zFvbPls
mfzbG6kbs2q/bnWkm5mX+oMa1gGBxjBktz64r/GR5uPe7UiF1CsfFBK/q+Uzgpnr
WT+6y2OxIa8cOWZPtNpnTHd6/GbpM+J20Krs3QhvV8y3YRj/BW/JAJQI/HEHI18m
jNBszfGgTWYgotqfZcgZM9dPbi63B7ZYbhD00gTUPKw2oj1+6zATvazy3cB6XasM
5APcWYqe6UOlc/mZH7iJ+OQuIzeroggdGYeNEoV4zF3IeyeJo9XHFm/+P3SZCQID
AQABoz8wPTAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBR4mvXf2gFYkWF IxCj
vMIItCRN7BTALBgNVHQ8EBAMCAQYwDQYJKoZIhvcNAQEFBQADggEBAJn1D+u9IYS2
bbW3Jl3gvbb/Fsp6QLoCT/xxxxXbctE4mQ2xSXfFmukUFL1GDbvKpgnbBRS220/J
Pafjb1fAIuivunOgIeJMoKAADAT820hUB48IdG9WDFwFI2U107XHZW2SsD7u/mPR
L+bynNhs6BqVRopjXgRIVyNdLcmFYIBNLV7xshLYpUeuCmZ1HD2xkODgBk5UcNnu
mKzeCM4h4CEVc79z+djnQA0sila3HpayHiKUfszpAprnpeDwcQ8VGsFQZwzV53m/
+mBc0kpQVLgN/DoCCWtYc1jFuTleY+Iz8kCzVSM6QlIarIcIE1p/mjCQKPsMfM7y
coe358PnPcU=
-----END CERTIFICATE-----
</ca>

remote-cert-tls server
key-direction 1
<tls-auth>

```

```

.....
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
7e76e4562b001b50ab1c3fae9710f9c0
9405c3915dfea681210ca2f1290a7383
a9b2c153a7548374a4d6ad25325c3579
cefd0c9a20426ca96077811b7e40df49
1b37829b866dd027f0855bd0b9326206
68db25bfb3b11a70469fe8f100970993
23adca22708ed4e1afce43e3137f041b
fee8278e3710d0ae3b63720b0b81fc12
7937020679b9e56b55d8e4b240942ea7
1bf5969181e102e07b4f4b285e6cb0ed
0acc1998f8fb3a1c439cc2300eb77043
3d39bc5502a6d1a6b46f2ee193b68767
1cbf12cd7472e2d31f3f52e73fa487f0
1bd7a1a8d57e23cd57fb43532624df2a
7584f316a0d7268a60ec15e419293523
9060b8c2cb98459e594f006ec9b40159
-----END OpenVPN Static key V1-----
</tls-auth>
cryptoapicert "SUBJ:MyClient1"
    
```

Note: If <tls-auth> key is missing in the client configuration file then it is likely because the Netscape Cert Type is used in the G500 Server Certificate. Refer to step 11 section 3.1.1 Generating a G500 Server Certificate on page 16 for how to remove Netscape Cert Type from the G500 Server Certificate. Server & Client Certificate Generation You also would need to remove the Netscape Cert Type from the Client Certificate. Refer to step 11 in section 3.1.2 on page 21 for how to remove Netscape Cert Type from the Client Certificate.

8. Revoking a Client certificate

All certificates are issued for a restricted time period of validity. However, it can happen that a certificate should not be used or has become invalid before its expiry date. In this case, the issuing CA should revoke this certificate by putting it on the list of revoked certificates (CRL) and publishing it.

Together with a private key and a certificate, a client device can prove its identity to the G500. If a malicious user ever discovered your private key, the malicious user would be able to access the G500 masquerading as you. The moment you are aware of a security breach that may involve the private key, you should revoke the associated certificate. If a certificate is revoked, the G500 does not accept any connections that use a revoked certificate.

Another reason for revoking a certificate may be that the owner of the certificate has left the company and no longer needs to connect to the G500. Revoking the certificate prevents that person from accessing the G500 even if the person retained his or her private key.

To revoke a certificate:

1. Revoke the certificate on the CA 8.1.
2. Generate a new Certificate Revocation List (CRL) – See section 8.2.
3. Install the CRL on the G500 – See section 8.3.
4. OpenVPN server configuration, Save and Commit changes to reflect new CRL changes.

8.1 Revoking the Certificate in XCA

To revoke the certificate in XCA:

1. Launch XCA from the Windows Programs menu.
2. In the tree view under the **Certificates** tab, open the branch containing your Certificate Authority.
3. Select and right-click the Client certificate to be removed (e.g., MyName).
4. Click **Revoke** option from the right-click menu.
5. Provide the date of revocation under field **Invalid Since** and reason for revocation from the dropdown list **Revocation Reason**.
6. Click **OK**.

8.2 Exporting the CRL in XCA

To export the CRL in XCA:

1. In the tree view under the **Certificates** tab, right-click the branch containing your Certificate Authority (e.g., MyCA).
2. Select the **CA** option in the right-click menu, and then option **Generate CRL**.
3. Under the **Dates** section, leave the **last update** as today's date.

4. Choose a date for **next update** when you want to update CRL next time to the G500s. If there is no planned date for next update, you can choose the expiry date of CA certificate as date for **next update**. Note: you can optionally use **Year/Month/Day** field and **Apply** to quickly change next update date.
5. Change the dropdown **Hashing Algorithm** to **SHA 256**.
6. Under the **Extensions**, leave the fields **CRL Number** and **Revocation reasons** checked. Leave the field **Authority key identifier** unchecked.
7. Click **OK**.
8. Under the **Revocation List** tab, select the CRL labelled as your Certificate Authority (e.g., MyCA). Verify that **Next update** field is set to what you have chosen in step 4.
9. Click **Export**.
10. In the dialog that appears, ensure the **Export Format** field is set to PEM. Browse to a protected location (e.g., My Documents->MyXCAFiles) and click **Save**. The file is named based upon the internal name of your CA with a ".pem" extension. Append "_CRL" to filename to indicate that this file is a CRL (e.g., MyCA_CRL.pem). Finally click **OK**.

8.3 Installing the CRL in the G500

To install the CRL in the G500:

1. Copy the CRL file generated in section 8.2 to one of two locations:
 - The folder /mnt/user/SecureScadaTransfer on the G500. In this case, use an SFTP/SCP file transfer program such as WinSCP or Secure File Browser from DS Agile MCP Studio (Refer to Appendix B in SWM0101 for details).
 - The directory \SecureScadaTransfer on a USB drive.
2. If you are using the USB drive method of transferring the files, insert the drive into any USB slot on the G500.
3. Connect to the G500 with a browser and click the Utilities tab under Settings options from the power bar.

Note: This Option is available in Utilities Tab under Settings option from Local HMI or from the Connected Mode in DS Agile MCP Studio only.
4. Click the **Import** button. You should see a dialog indicating that 1 CRL was successfully imported. Click **OK** to dismiss the dialog.
5. Click the **Manage** button, and then click the **CRL** tab.

Result: A dialog appears showing the CRL details in the Staged CRLs area.
6. Select the CRL and click **Install**.

Result: The CRL moves into the Installed CRLs area.
7. Close the dialog and log out of the G500.

9. Running OpenVPN Client as Windows Service using NSSM

Download the latest version of NSSM (Non-Sucking Service Manager) from link:

<http://nssm.cc/download>

NOTICE

The following procedure is reproduced with permission from Peter Senft at <http://www.rfc3092.net/>. Peter's original blog can be found at <http://www.rfc3092.net/2015/08/openvpn-windows-service-foo/>.

9.1 How to install NSSM

NSSM does not come with a Windows Server 2012 R2 installer.

To install NSSM:

1. Create a folder; for instance, in your "Program Files" directory (or whatever directory name %PROGRAMFILES% represents).
2. Depending on your operating system, copy the win32 or win64 version of <nssm.exe> into the Program Files directory.
3. Open a console window with administrator rights.
4. Navigate to the newly created folder.
5. Execute NSSM install file. For example:
C:\Program Files\NSSM>nssm.exe
NSSM: The non-sucking service manager
Version 2.24 64-bit, 2014-08-31

9.2 How to Use NSSM

Usage: nssm [<args> ...]

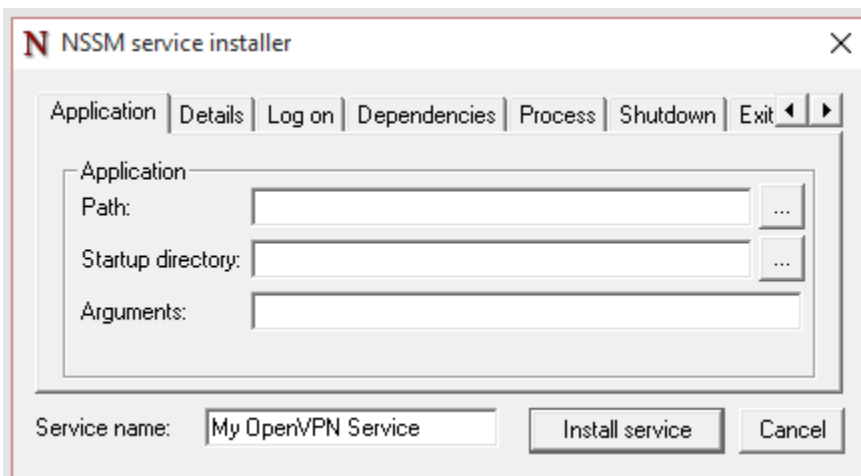
- To show service installation GUI:
nssm install [<servicename>]
- To install a service without confirmation:
nssm install <servicename> <app> [<args> ...]
- To show service editing GUI:
nssm edit <servicename>
- To retrieve or edit service parameters directly:
nssm get <servicename> <parameter> [<subparameter>]
nssm set <servicename> <parameter> [<subparameter>]
nssm reset <servicename> <parameter> [<subparameter>]

- To show service removal GUI:
nssm remove [<servicename>]
- To remove a service without confirmation:
nssm remove <servicename> confirm
- To manage a service:
nssm start <servicename>
nssm stop <servicename>
nssm restart <servicename>
nssm status <servicename>
nssm rotate <servicename>

9.3 Running OpenVPN as Windows Service Using NSSM

To run OpenVPN as a Windows service using NSSM:

1. Go to the NSSM folder using the Windows Command Line with administrator access:
C:\Program Files\NSSM>
2. Run the OpenVPN client as Service, execute the following command:
nssm install "My OpenVPN Service"
The NSSM service installer window Application tab appears.



9.4 Setting Up OpenVPN as a Service

To set up OpenVPN as a service:

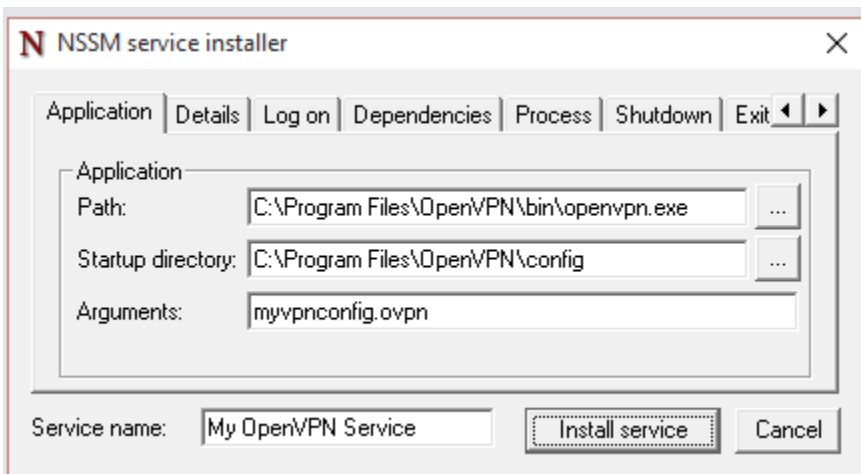
1. Complete the **Application** tab fields.

Path: This is the path to the OpenVPN binary and should usually be C:\Program Files\OpenVPN\bin\openvpn.exe.

Startup directory: This is the path to the directory where you store your OpenVPN configuration files. Usually that is C:\Program Files\OpenVPN\config. But if you want to run the OpenVPN UI with manual started tunnels in parallel, then create a separate folder, e.g., C:\Program Files\OpenVPN\config-nssm. Otherwise it is easy to confuse manual tunnels with service tunnels.

In this example, since manual tunnels are being used, use the default values.

Arguments: This is the configuration file for the tunnel, that should reside in the above defined startup directory.

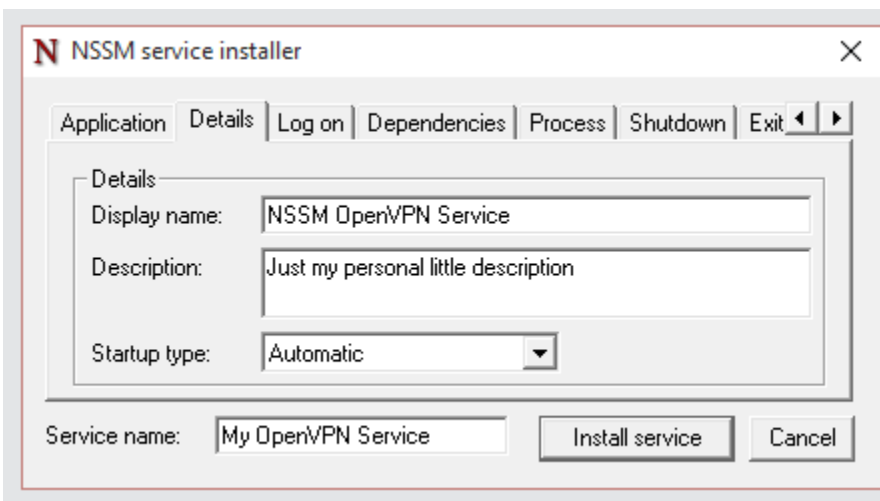


2. Complete the **Details** tab fields.

Display name: This is the name that is basically visible everywhere. The name is editable, but most of the time this is the same as the service name.

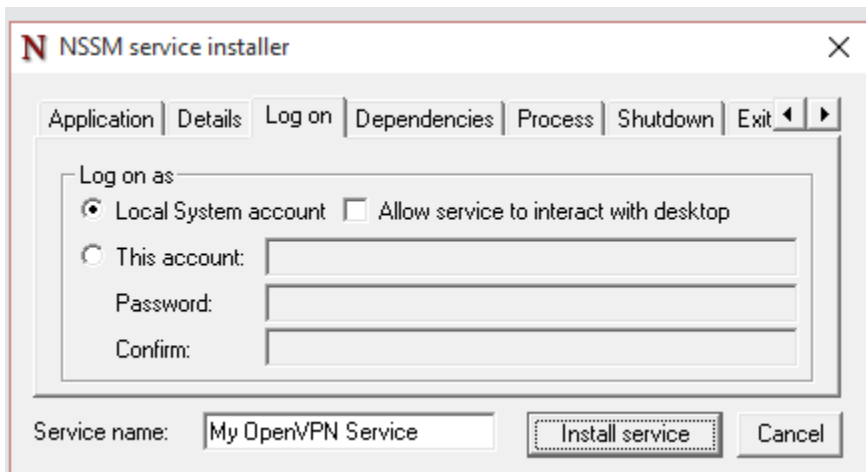
Description: This is the description that can be viewed later in the services area.

Start-up type: This is the standard service start up type setting for a window. Most likely choose Automatic here. But here user have the choice between Automatic, Automatic (Delayed Start), Manual and Disabled.



3. Complete the **Log On** tab fields.

Define how this service needs to run. Unless you are doing something unusual here, you can leave the default settings unchanged (that is, **Local System account**).



4. Complete the **Update** tab fields.

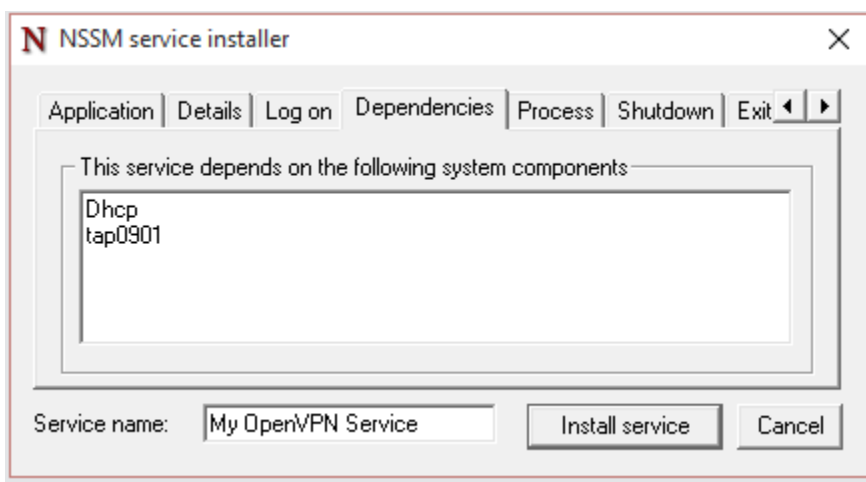
If running Windows 10, this tab can be important. Using the system account, you are able to install the service, but when starting the service, you might see an error. In the event log, the following message appears:

Program C:\Program Files\OpenVPN\bin\openvpn.exe for service OpenVPN siteopsvpn (NSSM) exited with return code 3221225794.

This means, that you used an account that has no rights to execute OpenVPN. This can be resolved by running the service as a user that has administrative rights on that computer.

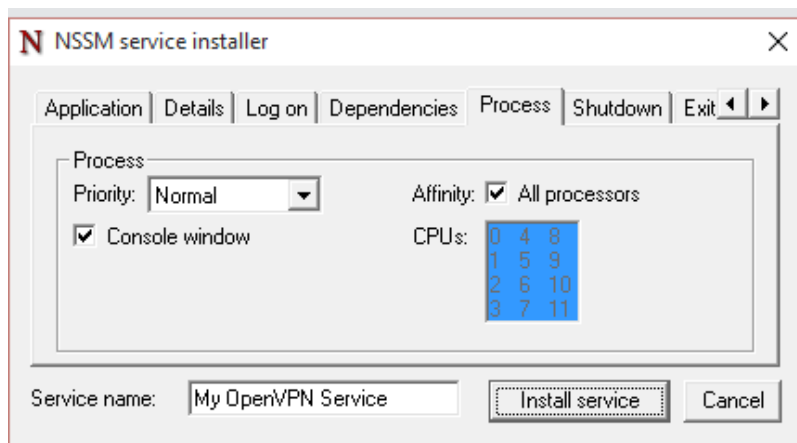
5. Complete the **Dependencies** tab fields.

Add the services that OpenVPN is depending on (Dhcp and tap0901).



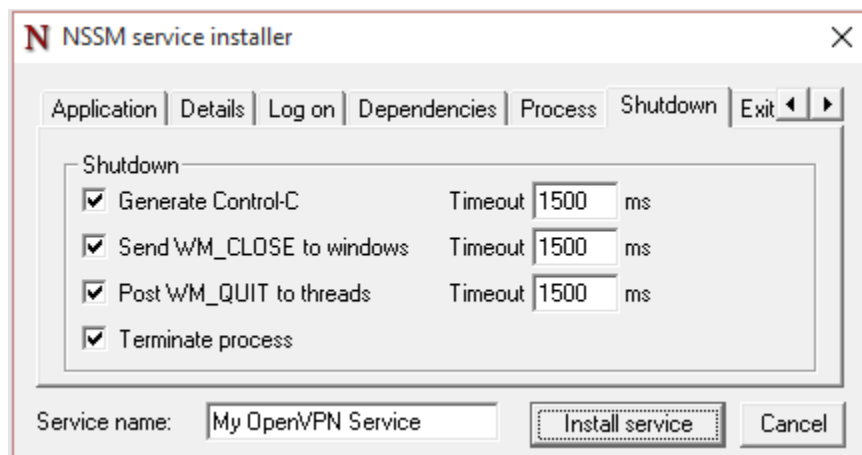
- Complete the **Process** tab fields.

In this tab, you can control how the service is handled by the processor. For instance, if it should only run on a specific processor or as a higher priority. For the normal use case this can be remain unchanged.



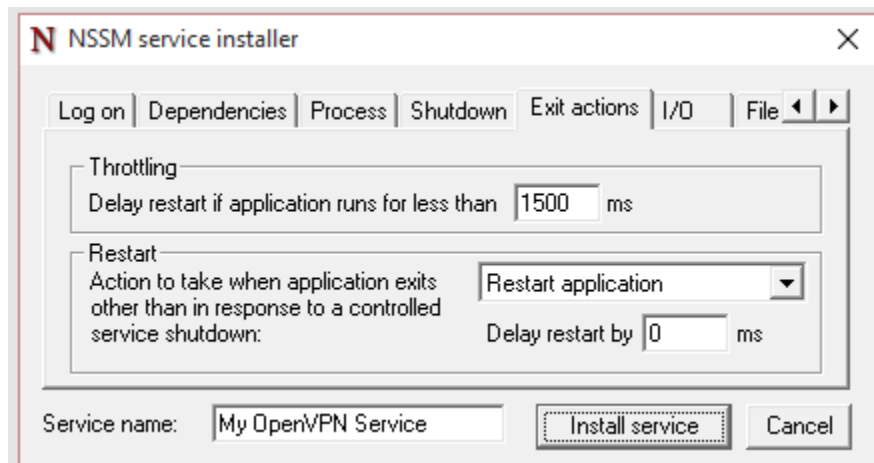
- Complete the **Shutdown** tab fields.

Under normal circumstances, no changes are required for this tab.



- Complete the **Exit Actions** tab fields.

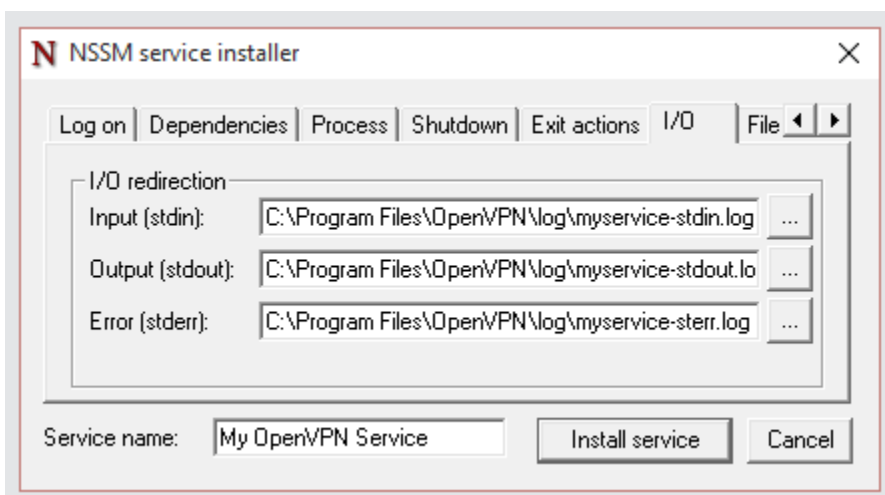
Under normal circumstances, no changes are required for this tab.



9. Complete the **I/O** tab fields.

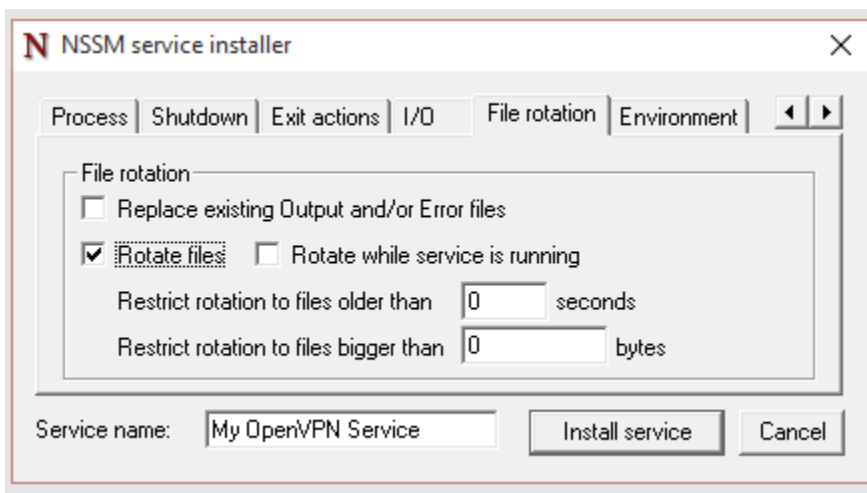
With the OpenVPN UI you can view the log files. However, with services you cannot view the logs, unless you define them here. Log files are usually located in:

C:\Program Files\OpenVPN\log.



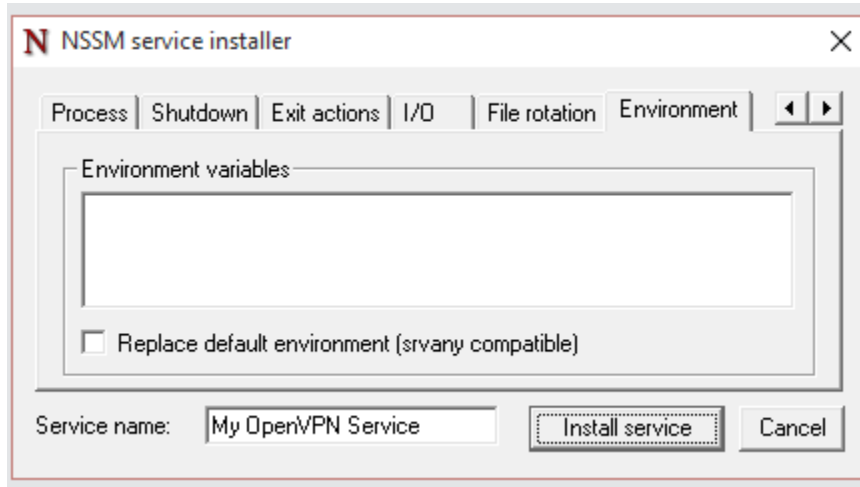
10. Complete the **File Rotation** tab fields.

This tab is an extension of the I/O tab, as it configures the log rotation.



11. Complete the **Environment** tab fields.

This last tab can usually be ignored. However, it can be useful if you want to add or even replace the environment.



12. Click **Install service**.

Result: NSSM installs OpenVPN as a service that can survive standby and sluggish network connections.

13. Start the newly created service with the:

- **net** command,
- **nssm** command, or
- Services in the control panel.

If you want to change anything, this can be done by calling NSSM with the edit parameter.

nssm edit "My OpenVPN Service"

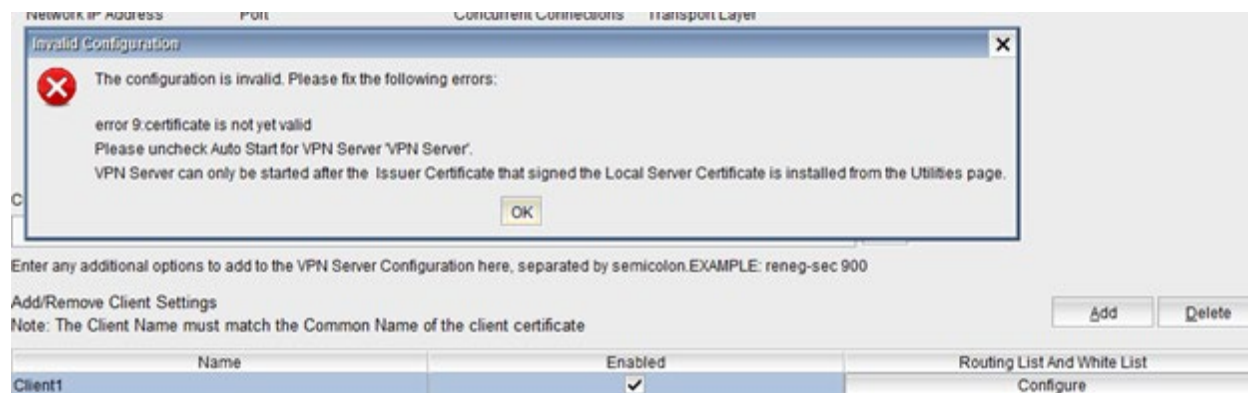
And, as previously stated, you can perform changes from the command line. The command sequence is:

```
nssm install "My OpenVPN Service" C:\Program Files\OpenVPN\bin\openvpn.exe
nssm set "My OpenVPN Service" AppDirectory "C:\Program Files\OpenVPN\config"
nssm set "My OpenVPN Service" AppParameters myvpnconfig.ovpn
nssm set "My OpenVPN Service" AppStdin "C:\Program Files\OpenVPN\log\myservice-stdin.log"
nssm set "My OpenVPN Service" AppStdout "C:\Program Files\OpenVPN\log\myservice-stdout.log"
nssm set "My OpenVPN Service" AppStderr "C:\Program Files\OpenVPN\log\myservice-stderr.log"
nssm set "My OpenVPN Service" AppRotateFiles 1
nssm set "My OpenVPN Service" DependOnService Dhcp tap0901
```

A. Certificate Error Messages Logged by OpenVPN Configuration HMI

This appendix describes possible error messages logged by the OpenVPN configuration HMI for errors in certificates.

Example Error Message:



List of Error Codes from OpenSSL.org:

Error Code	Description
0 X509_V_OK: ok	The operation was successful.
2 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT: unable to get issuer certificate	The issuer certificate of a looked-up certificate could not be found. This normally means the list of trusted certificates is not complete. Ensure that Issuer Certificate for the Installed Local Certificate exists. Also ensure that all certificates in the Issuer Certificate chain are installed in the G500.
3 X509_V_ERR_UNABLE_TO_GET_CRL: unable to get certificate CRL	The CRL of a certificate could not be found.
4 X509_V_ERR_UNABLE_TO_DECRYPT_CERT_SIGNATURE: unable to decrypt certificate's signature	The certificate signature could not be decrypted. This means that the actual signature value could not be determined rather than it not matching the expected value, this is only meaningful for RSA keys.

Error Code	Description
5 X509_V_ERR_UNABLE_TO_DECRYPT_CRL_SIGNATURE: unable to decrypt CRL's signature	The CRL signature could not be decrypted: this means that the actual signature value could not be determined rather than it not matching the expected value. Unused.
6 X509_V_ERR_UNABLE_TO_DECODE_ISSUER_PUBLIC_KEY: unable to decode issuer public key	The public key in the certificate SubjectPublicKeyInfo could not be read.
7 X509_V_ERR_CERT_SIGNATURE_FAILURE: certificate signature failure	The signature of the certificate is invalid.
8 X509_V_ERR_CRL_SIGNATURE_FAILURE: CRL signature failure	The signature of the certificate is invalid.
9 X509_V_ERR_CERT_NOT_YET_VALID: certificate is not yet valid	The certificate is not yet valid: the notBefore date is after the current time. This issue could be caused by an incorrect time on the G500. Ensure that the G500 time is correct. An incorrect time could occur if the G500 is configured for the UTC timezone but its time is set to a non-UTC local time. It is recommended that the G500 timezone be set to the correct local timezone and time corrected in this case.
10 X509_V_ERR_CERT_HAS_EXPIRED: certificate has expired	The certificate has expired: that is the notAfter date is before the current time.
11 X509_V_ERR_CRL_NOT_YET_VALID: CRL is not yet valid	The CRL is not yet valid.
12 X509_V_ERR_CRL_HAS_EXPIRED: CRL has expired	The CRL has expired.
13 X509_V_ERR_ERROR_IN_CERT_NOT_BEFORE_FIELD: format error in certificate's notBefore field	The certificate notBefore field contains an invalid time.
14 X509_V_ERR_ERROR_IN_CERT_NOT_AFTER_FIELD: format error in certificate's notAfter field	The certificate notAfter field contains an invalid time.
15 X509_V_ERR_ERROR_IN_CRL_LAST_UPDATE_FIELD: format error in CRL's lastUpdate field	The CRL lastUpdate field contains an invalid time.
16 X509_V_ERR_ERROR_IN_CRL_NEXT_UPDATE_FIELD: format error in CRL's nextUpdate field	The CRL nextUpdate field contains an invalid time.
17 X509_V_ERR_OUT_OF_MEM: out of memory	An error occurred trying to allocate memory. This should never happen.
18 X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT: self-signed certificate	The passed certificate is self-signed, and the same certificate cannot be found in the list of trusted certificates.

Error Code	Description
19 X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN: self-signed certificate in certificate chain	The certificate chain could be built up using the untrusted certificates, but the root could not be found locally.
20 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY: unable to get local issuer certificate	The issuer certificate could not be found: this occurs if the issuer certificate of an untrusted certificate cannot be found. Ensure that Issuer Certificate for the Installed Local Certificate exists. Also ensure that all certificates in the Issuer Certificate chain are installed in the G500.
21 X509_V_ERR_UNABLE_TO_VERIFY_LEAF_SIGNATURE: unable to verify the first certificate	No signatures could be verified because the chain contains only one certificate and it is not self-signed.
22 X509_V_ERR_CERT_CHAIN_TOO_LONG: certificate chain too long	The certificate chain length is greater than the supplied maximum depth. Unused.
23 X509_V_ERR_CERT_REVOKED: certificate revoked	The certificate has been revoked.
24 X509_V_ERR_INVALID_CA: invalid CA certificate	A CA certificate is invalid. Either it is not a CA, or its extensions are not consistent with the supplied purpose.
25 X509_V_ERR_PATH_LENGTH_EXCEEDED: path length constraint exceeded	The basic Constraints path length parameter has been exceeded.
26 X509_V_ERR_INVALID_PURPOSE: unsupported certificate purpose	The supplied certificate cannot be used for the specified purpose.
27 X509_V_ERR_CERT_UNTRUSTED: certificate not trusted	The root CA is not marked as trusted for the specified purpose.
28 X509_V_ERR_CERT_REJECTED: certificate rejected	The root CA is marked to reject the specified purpose.
29 X509_V_ERR_SUBJECT_ISSUER_MISMATCH: subject issuer mismatch	The current candidate issuer certificate was rejected because its subject name did not match the issuer name of the current certificate. Only displayed when the -issuer_checks option is set.
30 X509_V_ERR_AKID_SKID_MISMATCH: authority and subject key identifier mismatch	The current candidate issuer certificate was rejected because its subject key identifier was present and did not match the authority key identifier current certificate. Only displayed when the -issuer_checks option is set.

Error Code	Description
31 X509_V_ERR_AKID_ISSUER_SERIAL_MISMATCH: authority and issuer serial number mismatch	The current candidate issuer certificate was rejected because its issuer name and serial number was present and did not match the authority key identifier of the current certificate. Only displayed when the -issuer_checks option is set.
32 X509_V_ERR_KEYUSAGE_NO_CERTSIGN:key usage does not include certificate signing	The current candidate issuer certificate was rejected because its keyUsage extension does not permit certificate signing.
50 X509_V_ERR_APPLICATION_VERIFICATION: application verification failure	An application specific error. Unused.

B. OpenVPN Server Log Messages

This appendix describes common error or info messages logged by OpenVPN server log that can be used to troubleshoot the connectivity issues between VPN server and client.

VPN Server Log Message(s)	Cause of the issue and recommended actions
<p>2017-05-07T08:33:36.597083+00:00,00000000,597,None,openvpn:N9219:ERR -: Cannot load CA certificate file [[INLINE]] (no entries were read),</p>	<p>Check INLINE CA entry(ies) are not properly embedded into either VPN Server (/etc/openvpn/ovpn-server.conf) or Client configuration files. Following is an example of a correctly embedded INLINE ca entry:</p> <pre><ca> -----BEGIN CERTIFICATE----- MIIDxTCCAq2gAwIBAgIBATANBgkqhkiG9w00BAQUFADB 8MQswCQYDVQQGEwJDQTEL ... PG0MFqakCdoorEfVtsI73wSd5z+76fiOUcQF+JsXPBgYO 2IY7TcCSNAf592tZC1w y22boL1ndWIC -----END CERTIFICATE----- </ca></pre> <p>Following is an example of an invalid (empty) entry:</p> <pre><ca> </ca></pre> <p>If an invalid or empty INLINE CA entry exists, contact GE Grid Solutions Technical Support for further assistance.</p>
<p>2017-05-07T08:41:25.710242+00:00,00000000,710,None,openvpn:N13694:ERR -: Insufficient key material or header text not found in file '[[INLINE]]' (0/128/256 bytes found/min/max),</p>	<p>Check INLINE <tls-auth> key is not properly embedded into either VPN Server (/etc/openvpn/ovpn-server.conf) or Client configuration files. Following is an example of correctly embedded INLINE <tls-auth> key entry.</p> <pre><tls-auth> # # 2048 bit OpenVPN static key # -----BEGIN OpenVPN Static key V1----- ddd5343a60c7313f2e0c1e0531533047 f1578505715790cdb02e3548d4353fd0 -----END OpenVPN Static key V1----- </tls-auth></pre> <p>Following is an example of an invalid (empty) entry:</p> <pre><tls-auth> </tls-auth></pre> <p>If an invalid or empty <tls-auth> key exists, contact GE Grid Solutions Technical Support for further assistance.</p>

<p>2017-05-07T08:55:45.750417+00:00,00000000,750,None,openvpn:N20901:ERR -: Cannot load CA certificate file [[INLINE]] (no entries were read),</p>	<p>Check if INLINE CA entry(ies) embedded in the VPN Server (/etc/openvpn/ovpn-server.conf) and Client configuration files are the same.. If not, try exporting the Client configuration again from the G500 Utilities tab under Settings option.</p>
<p>2017-05-07T09:01:11.621226+00:00,00000000,621,None,openvpn:N24633:ERR -: INLINE tls-auth file lacks the requisite 2 keys,</p>	<p>Check INLINE <tls-auth> key embedded in the VPN Server (/etc/openvpn/ovpn-server.conf) or Client configuration files are same. If different, try exporting the Client configuration again from the G500 Utilities tab under Settings option.</p>
<p>2017-05-07T01:21:23.203099+00:00,00000000,203,None,openvpn:N15234:NOTICE -: 172.12.233.68:63308 TLS: Initial packet from [AF_INET]172.12.233.68:63308, sid=2ee6fb0da06dc8a0,</p>	<p>Check if the client certificate is revoked. In this case you would need to create a new client certificate with the same common name. (Or) Check if the Client (.p12) certificate is not properly created (e.g., different CA than used by G500 Server certificate, mismatched common name etc..) or not properly installed in the client. Generate a new client certificate with the same common name and then install in the client.</p>
<p>2017-05-07T09:07:07.298309+00:00,00000000,298,None,openvpn:N28913:NOTICE -: 172.12.233.68:57360 SENT CONTROL [MyClient]: 'AUTH_FAILED' (status=1),</p>	<p>Check the Client is Disabled in configuration for openvpn server in G500. If so, enable the Client. (Or) Check the common name of Client certificate is the same as the client name in the configuration for the OpenVPN server in the G500. If not, correct the Client name in the OpenVPN server configuration.</p>

C. VPN Client from Ubuntu PC

To integrate the OpenVPN client running in Ubuntu 16.04LTS with the G500:

1. Setup your CA – see section 2.1.2 .
2. Generate Diffie Hellman (DH) parameters; see Chapter 2.
3. Generate private keys and certificates for your G500; see section 3.1.1 .
4. Generate client certificate + private key in .pem format for OpenVPN client that runs in Ubuntu 16.04LTS PC.
5. Install the CA's Certificate on your G500; see section 4.1.
6. Install the private keys, certificates and optional Diffie Hellman parameters on your G500; see section 4.1
7. Copy the .pem client certificate + private key into `"/etc/openvpn/"` folder or any other location to which openvpn client can have an administrator privileges.
8. Using the "Export VPN Client File" option in Utilities tab under Settings option page, export the OpenVPN client configuration (*.ovpn) into a desired location; see section 5.2.
9. Securely copy the OpenVPN client configuration into `"/etc/openvpn/"` folder or any other location to which openvpn client can have an administrator privileges.
10. Open the VPN Client configuration file using "vi" or any other editor and do the below steps.

- Comment the line starts with "cryptoapicert" with "#" as shown below.

```
#cryptoapicert "SUBJ:MyCA_Client1"
```

- And, add the below two lines to the bottom of the file as shown below.

```
cert <Patch of MyCA_Client1.pem>/MyCA_Client1.pem
```

```
key <Patch of MyCA_Client1.pem>/MyCA_Client1.pem
```

e.g.:

```
cert </etc/openvpn/MyCA_Client1.pem
```

```
key </etc/openvpn/MyCA_Client1.pem
```

11. Save the Configuration file and Run the OpenVPN client software from Ubuntu 16.04LTS PC using the below command from the terminal.

```
sudo openvpn --config <path of the Client Config File>/ MyCA_Client1.ovpn file.
```

For example:

```
sudo openvpn --config /etc/openvpn/ MyCA_Client1.ovpn file.
```

12. Verify in G500 VPN Server Log that VPN channel is established between OpenVPN Client running in Ubuntu 16.04 LTS and G500.

D. List of Acronyms

Table 8 List of Acronyms

Abbreviation	Description
CA	Certification Authority
CN	Common Name
CRL	Certificate Revocation List
DCA	Data Collection Application
DHE	Diffie Hellman Ephemeral
DPA	Data Presentation Application
DTA	Data Translation Application
FQDN	Full Qualify Distinguished Name
HMAC	Hash-based Message Authentication Code
HMI	Human Machine Interface
IED	Intelligent Electronic Device
JVM	Java Virtual Machine
LAN	Local Area Network
NSSM	Non-Sucking Service Manager
OU	Organizational Unit
PEM	Privacy Enhanced Mail
PKCS	Public Key Cryptography
PKI	Public Key Infrastructure
PRF	Protective Relay Fault
RTDB	Real Time Data Base
RTU	Remote Terminal Unit
SDD	Software Design Document
SOE	Sequence of Event
SPT	Secure Pass-Through
SSDD	Software Subsystem Design Document
TLS	Transport Layer Security
VPN	Virtual Private Network
WAN	Wide Area Network
XCA	X Certificate and Key Management

MODIFICATION RECORD

Version	Revision	Date	Change Description
1.00	0	26 th March, 2019	Document Created.

