NatQuery
Secure FTP (FTPS) Configuration

Overview

With the release of NatQuery version 5.3.0, NatQuery has been enhanced to support both Secured File Transfer Protocol (FTPS) Implicit and Explicit processing, in addition to supporting normal FTP communication to remote platforms.

For a number of years, NatQuery supported FTP operations against a remote platform by utilizing a Microsoft Dynamic Link Library (DLL) called WININET that was provided with an installation of Microsoft Internet Explorer (IE). As IE was typically found on all client machines, this re-use of an already existing component was beneficial to both NatWorks and our customers.

In response to the need by customers to support Secured FTP, a protocol not provided by WININET.DLL, NatQuery's reliance and utilization of WININET.DLL has ended in favor of using a software component product called PowerTCP provided by Dart Communications. With the adoption of PowerTCP, NatQuery can now support communication with any standard FTP or secure FTP (FTPS) which supports SSL 2.0, SSL 3.0, PCT and TLS; with the PowerTCP component being provided as part of a NatQuery installation royalty-free.

In a typical FTP environment, a FTP user only has to have an authorized USER-ID and Password in order to conduct automated basic FTP operations such as PUT or GET from a client workstation to a remote server. Once the FTP client is given a valid and authorized USER-ID and Password, the client machine can connect to the remote FTP Server, thus allowing data to be moved back and forth between a client machine and a host machine. The problem with using basic FTP is that all data being moved is un-encrypted, such that it could be possible for someone to intercept the command and data being passed.

With Secure FTP (FTPS) however, commands and data can both be encrypted, and therefore many customers are adopting this form of communication between clients and servers.

A fundamental difference between using FTP versus Secured FTP (FTPS) is that in an FTPS environment and in addition to requiring a valid and authorized USER-ID and Password – the client and server must "Trust" each other, with this "trust" being accomplished by way of Certificates that are issued by a Certificate Authority (CA). Subsequent to creating a Certificate, which is stored in a digital file, the CA will provide this file to the users requiring FTPS access. The Certificate is then imported onto the client machine(s) where it is then stored within the Windows Registry. When the Client then establishes an FTPS connection, the local Certificate is utilized to verify the credentials of the Server, and likewise the Server machine is able to verify the credentials of the User, after which encryption is then used for all data throughput.

The purpose of this document then is to guide a user through the process of configuring NatQuery to utilize FTPS as opposed to using basic FTP.

Configuring NatQuery to use FTPS

Under normal operations where NatQuery will use FTP or FTPS to communicate to the platform upon which Software AG's NATURAL and ADABAS reside, NatQuery needs to be initially given configuration information to support this communication.

In addition to communicating to the NATURAL / ADABAS Server, NatQuery is additionally able to automatically load extracted data into specific Relation Database Management Systems (RDBMS), and since the RDBMS is likely to reside on a completely different platform; this communication may also require the use of FTP or FTPS and therefore also need to be configured.

This section therefore covers the topic of Configuring NatQuery to use FTPS against the remote NATURAL / ADABAS source platform, with a subsequent section covering the topic of Configuring NatQuery to use FTPS against a remote RDBMS target platform.

An additional section covers how to handle Certificates for either configuration.

Configuring NatQuery to use FTPS with the ADABAS Server Platform

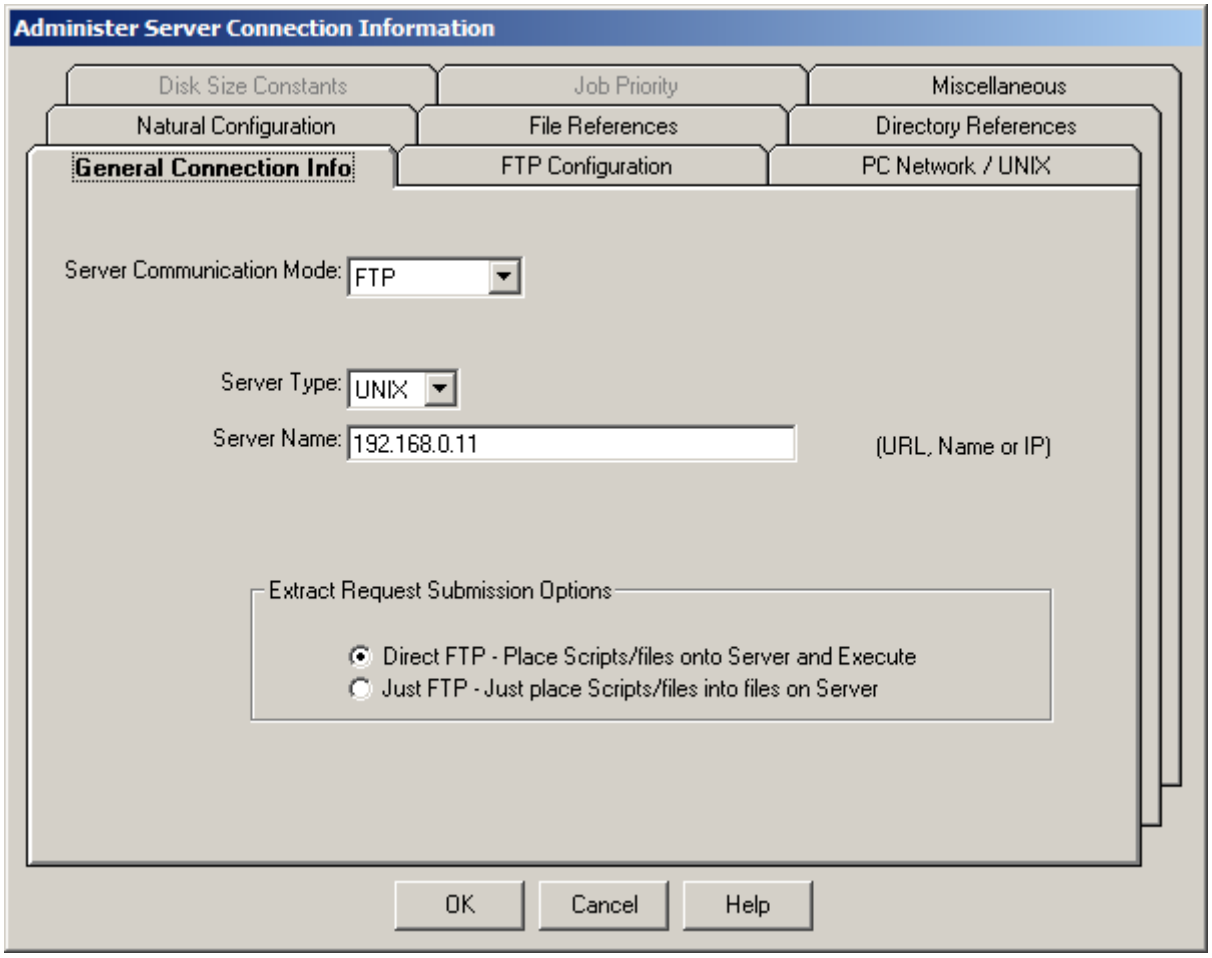
This section describes the steps needed to configure NatQuery to use a Secure FTP connection against the platform upon which NATURAL / ADABAS resides.

To configure NatQuery to use Secure FTP against the remote NATURAL / ADABAS platform, perform the following steps (these steps assume that the version of NatQuery being used has been given an Administrator License Key).:

1) **Start NatQuery**
   Please start NatQuery if it is not already started. If already started, insure that NatQuery is open with an empty NatQuery desktop (I.E. no Query windows or other windows open).

2) **Invoke the Administer Server Connection Information Window**
   On an empty NatQuery desktop, click **Administer** > **Environment Configuration** > **Server Connection Configuration** > **Server Information**. This action will invoke the Administer Server Connection Information window.

3) **Configure FTP – Step 1 – General Connection Information Tab**
   The Administer Server Connection Information window provides for Multiple Tabs along the top, and by default, the General Connection Info tab will be displayed. This Tab will look like the following image:



a. **Server Communication Mode**
Set the Server Communication Mode to be the desired communication Mode. Possible values are “PC Network”, “FTP” and “none”.

If Secured FTP communication is desired, then this value should be set to “FTP”.

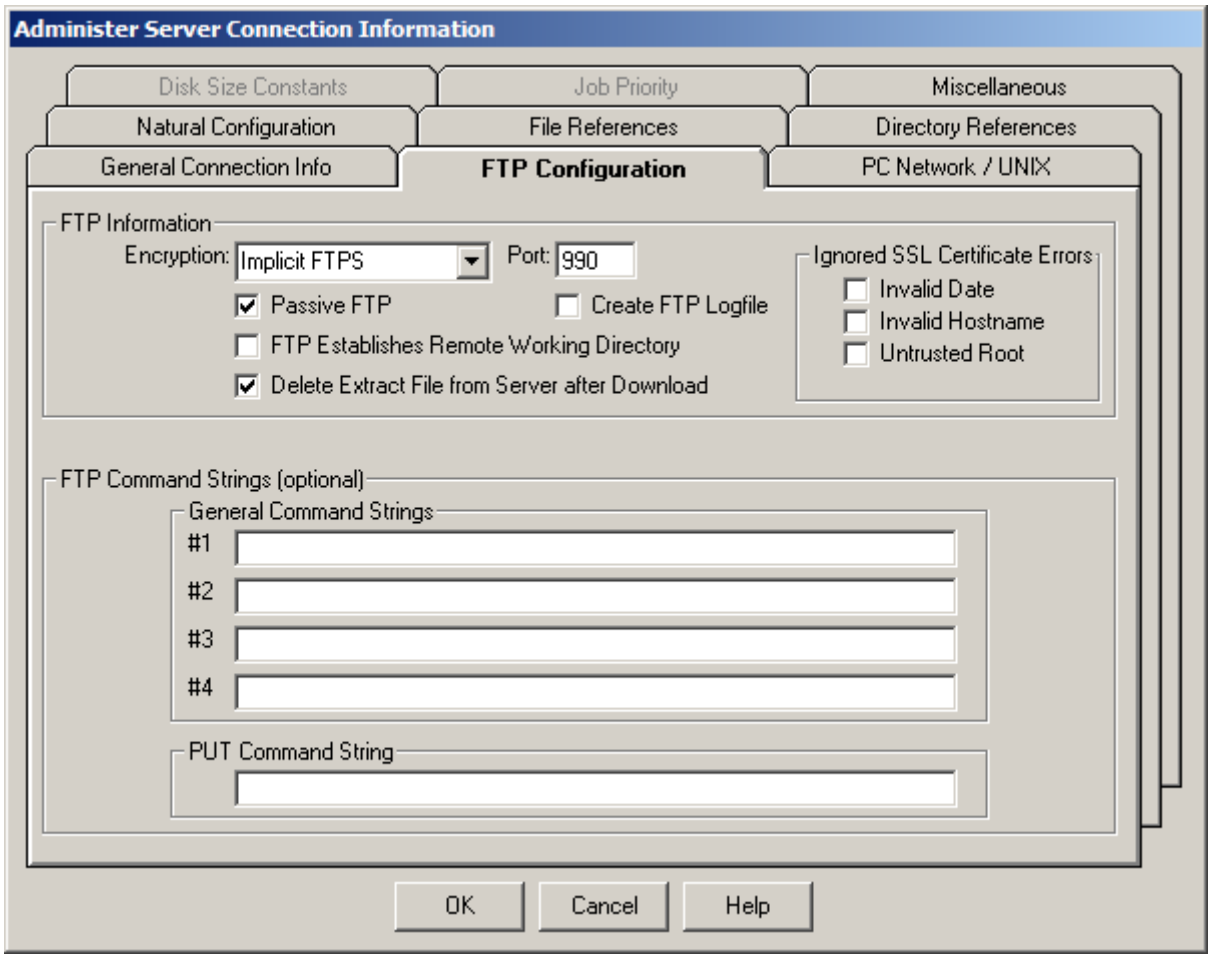
b. **Server Type**
Insure that the Server Type is set to the appropriate value for the platform upon which the NATURAL / ADABAS Server resides. Value can be “MVS”, “VSE”, “UNIX” or “NT”.

c. **Server Name**
Set the Server Name to be the Universal Resource Locator (URL), Name or IP Address of the platform upon which the NATURAL / ADABAS Server resides.

d. **Extract Request Submission Options**
These checkboxes control how FTP operations will interact with the Remote

Server. Please refer to the NatQuery Installation & Operations Manual for a full description of these controls and what they do.

4) **Configure FTP – Step 2 – FTP Configuration Tab**
While remaining on the Administer Server Connection Information window, click the FTP Configuration Tab. The Tab will look like the following image:



a. **FTP Information Frame**

i. **Encryption**
This should be set to the type of FTP connection that is desired. Options are "None (Normal FTP)", "Implicit FTPS" and "Explicit FTPS"; select the type of FTP communication that matches the setting of the FTP Server on the remote NATURAL / ADABAS platform.

ii. **Port**
This should be set to the value of the Port on the remote FTP Server that will handle the FTP Connection. For normal FTP, this is usually "21", and in most cases will be "990" by default when FTPS Implicit or Explicit connections are used. Set the Port setting to the correct value.

iii. **Passive FTP**
If checked, this checkbox will enable Passive (PASV) FTP communication, if left unchecked Passive FTP communication will be disabled.

Usually, Passive FTP should be checked.

iv. Create FTP Logfile
This checkbox controls whether or not a Log File of FTP Operations is created when a user performs a FTP operation. This Log File can be useful when debugging connections issues, but should be disabled (unchecked) when FTP operations are working properly because a user's password **IS** recorded in the Log File.

When checked, a log file is created with the name of:

*userid*_FTP_Trace.Log

This file is created in the path specified by the NatQuery Environment Path, where "*userid*" is replaced with the User ID of the NatQuery user.

v. FTP Establishes Remote Working Directory
If this checkbox is not checked, then NatQuery will not attempt to do a "Change Directory" (CD) once a FTP connection is established – FTP operations will assume that the FTP connection has set the proper path into which files will be PUT and GET.

If this checkbox is checked, then after the FTP connection is established, NatQuery will perform a Change Directory operation through FTP to set the remote path to the value specified in the field "**Request File Directory**" on the **Directory References** Tab.

vi. Delete Extract File from Server after Download
If this checkbox is checked, then after NatQuery has downloaded an extract file from the FTP server to the FTP Client workstation, NatQuery will issue a DELETE against the remote file using FTP – thereby freeing up disk space on the server.

If this checkbox is not checked, then subsequent to a file being downloaded by FTP, nothing further occurs.

It is suggested that this file be checked so that disk space may be saved on the server platform.

vii. Ignored SSL Certificate Errors Frame

When a Secured FTP connection is established, the handshaking that occurs to verify the credentials of both the Client and the Server will check such things as the Date of the Certificate, the Host Name in the Certificate and whether or not the "Root" path is trusted.

Under normal circumstances, such Certificate Errors should NOT be ignored, such that a FTP should not be allowed if any such error occurs. To allow for continued operation even in the face of such errors, selecting the appropriate checkbox or checkboxes will cause NatQuery to ignore such errors and continue processing the FTP requests.

Usually, these checkboxes should all be left unchecked.

viii. FTP Command Strings Frame

The FTP Command Strings Frame allows for FTP Command strings to be inserted into FTP communications as General Commands (which will always be inserted) or PUT Command (which will be inserted as an FTP Command just before a PUT Operation is attempted).

For further information on FTP Command String usage, please refer to the NatQuery Installation and Operations Manual.

5) Complete FTP Configuration

With the above steps completed, secure FTP against the server platform should now be properly configured.

Click the **OK** button to close the **Administer Server Connection Information** window. As this window closes, you will be prompted to **Verify the Environment Configuration** with a pop-up messagebox.

Click **Yes** to this messagebox and then review the resulting **Verify Configuration Report**, which can then be closed by clicking its **OK** button.

6) Handle Secure FTP Certificate(s)

With the above steps complete, you can proceed to handle the Secure FTP Certificate(s) needed to complete the Secure FTP configuration against the source ADABAS platform; these are outlined in the section of this manual entitled **Handling Secure FTP Certificates**.

Configuring NatQuery to use FTPS against a RDBMS Target Platform

This section describes the steps needed to configure NatQuery to use a Secure FTP connection against the platform upon which a target RDBMS resides. Depending upon how your organization uses NatQuery / NatCDC this section may not be applicable; it will only be applicable if you are using NatQuery / NatCDC to extract data from ADABAS and load this data into a RDBMS residing on a completely separate platform.

To configure Secure FTP against a remote RDBMS platform, perform the following steps:

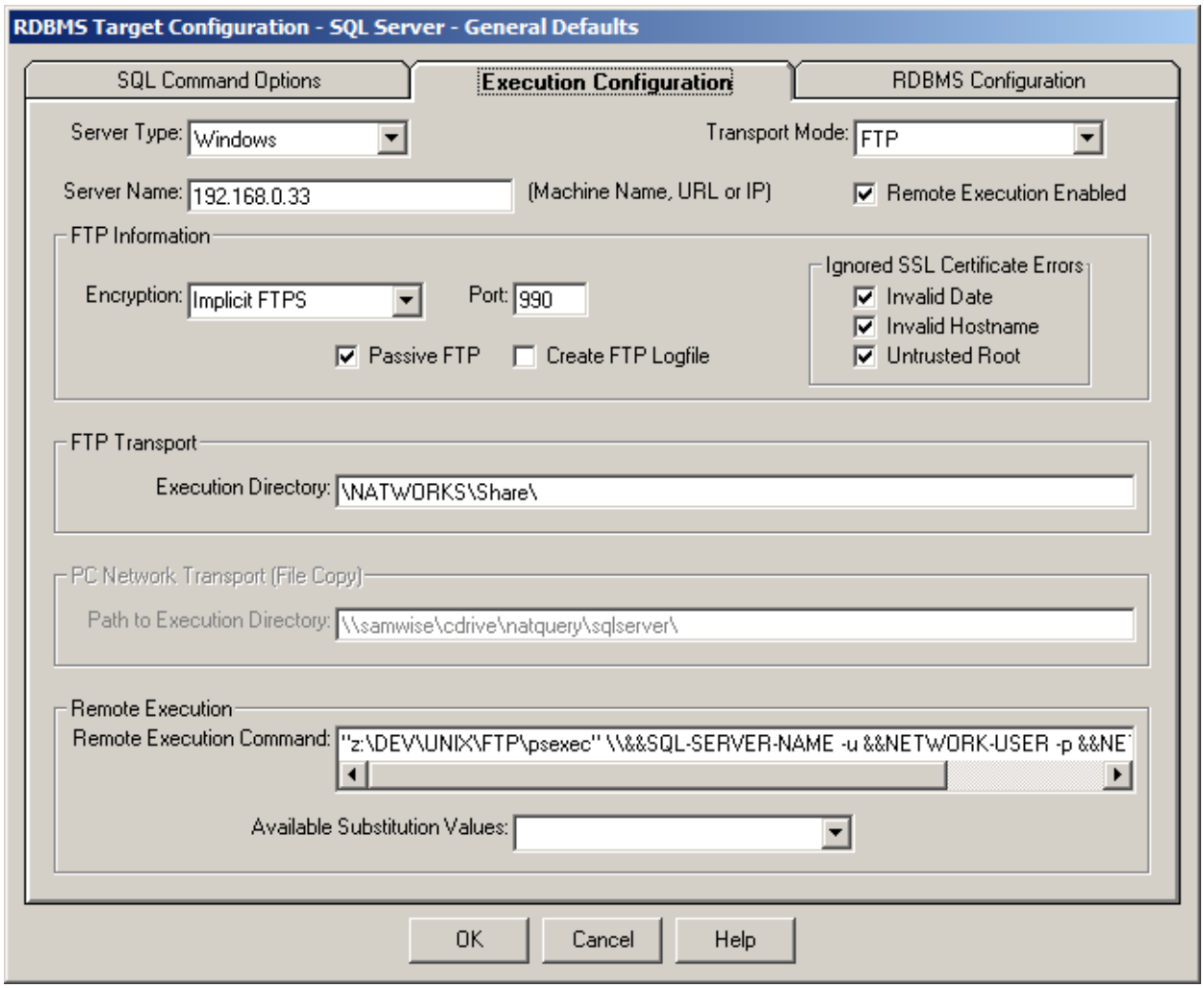
1. **Start NatQuery**
   Please start NatQuery if it is not already started. If already started, insure that NatQuery is open with an empty NatQuery desktop (I.E. no Query windows or other windows open).

2. **Invoke the Administer Server Connection Information Window**
   On an empty NatQuery desktop, click **Administer** > **Environment Configuration** > **RDBMS Target Configuration** > ***RDBMSName*** (where the "***RDBMSName***" is either "SQL Server", "MySQL" or "Oracle". This action will invoke appropriate **RDBMS Target Configuration – *RDBMSName* - General Defaults** window.

   When this window appears, the first Tab entitled ***RDBMSName*** **Command Options** (where ***RDBMSName*** is either "SQL Server", "MySQL".

   Click on the **Execution Configuration** Tab to continue.

3. **Configure FTP – Execution Configuration Tab**
   The Execution Configuration Tab provides for the capture of FTP related information. This tab will look like the following image:



a. **Server Type**
Set the Server Type to the value that represents the type of platform upon which the Target RDBMS resides. Possible values are “Windows” or “UNIX/Linux”.

b. **Transport Mode**
Set the Transport Mode to be the desired communication Mode. Possible values are “PC Network/Filecopy”, “FTP” and “none”.

If Secured FTP communication is desired, then this value should be set to “FTP”.

c. **Server Name**
Set the Server Name to be the Universal Resource Locator (URL), Name or IP Address of the platform upon which the RDBMS Server resides.

d. **Remote Execution Enabled**
This checkbox instructs NatQuery as to whether or not NatQuery will attempt to execute the NatQuery-generated processing scripts once they are placed into the target machine.

Further discussion on configuring Remote Execution is described in the NatQuery Installation and Operations Manual.

e. **FTP Information Frame**

i. **Encryption**
This should be set to the type of FTP connection that is desired. Options are “None (Normal FTP)”, “Implicit FTPS” and “Explicit FTPS”; select the type of FTP communication that matches the setting of the FTP Server on the remote RDBMS platform.

ii. **Port**
This should be set to the value of the Port on the remote FTP Server on the RDBMS target that will handle the FTP Connection.

For normal FTP, this is usually “21” and in most cases will be “990” by default when FTPS Implicit or Explicit connections are used.

Set the **Port** setting to the correct value.

iii. **Passive FTP**
If checked, this checkbox will enable Passive (PASV) FTP communication, if left unchecked Passive FTP communication will be disabled.

Usually, **Passive FTP** should be checked.

iv. **Create FTP Logfile**
This checkbox controls whether or not a Log File of FTP Operations is created when a user performs a FTP operation. This Log File can be useful when debugging connections issues, but should be disabled (unchecked) when FTP operations are working properly because a user’s password **IS** recorded in the Log File.

When checked, a log file with the name of:

*userid*_FTP_RDBMS_TRACE.Log

This file is created in the path specified by the NatQuery Environment

Path, where "*userid*" is replaced with the User ID of the NatQuery user.

f. **FTP Transport Frame**
The FTP Transport Frame contains a single field; **Execution Directory.**

The path value placed into this text field is relative to the Target RDBMS platform, and represents the directory that automated FTP will make a Change Directory to, and will additionally be used within the NatQuery-generated script so that execution of Load processes may function correctly.

Set this path to the relative path on the target RDBMS platform where FTPed files will be placed (scripts, parameter files, and data) for subsequent loading into the target RDBMS.

g. **Complete RDBMS Target FTP Configuration**
With the above steps completed, Secure FTP against the target RDBMS platform should now be properly configured.

Click the **OK** button to close the **Target Configuration – *RDBMSName* - General Defaults** window.

4. **Handle Secure FTP Certificate(s)**
With the above steps complete, you can proceed to handle the Secure FTP Certificate(s) needed to complete the Secure FTP configuration against the target RDBMS platform; these are outlined in the section of this manual entitled **Handling Secure FTP Certificates**.

Importing Secure FTP Certificates

When enabling Secure FTP connections, a client machine needs to be given the appropriate Certificate issued by a Certificate Authority (CA) for the platform being accessed. This Certificate is then stored internally in the Windows Registry where it is subsequently automatically accessed when Secure FTP Operations are executed.

If the appropriate Certificates are already installed into the Security Store on the Client Machine then this section may be bypassed.

In the current version of NatQuery, NatQuery itself does not provide any mechanism to Import a Certificate into the Windows Registry as this ability is already inherent in a Windows environment through a function available with Microsoft Internet Explorer and other browsers.

As Internet Explorer (IE) is typically available in every Windows installation, these instructions utilize IE as the mechanism to Import required Certificates.

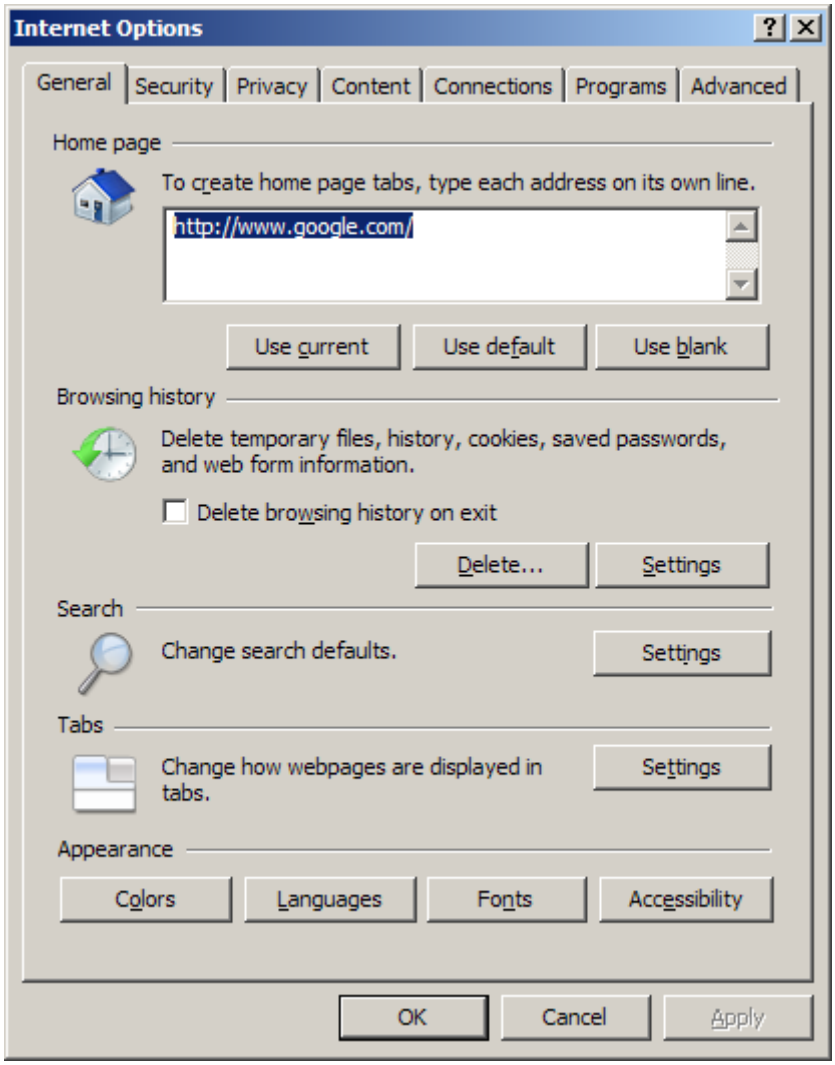
NOTE: The following process assumes that you have computer access to a digital Certificate created by a Certificate Authority that corresponds to the target FTP platform. If you do not have this Certificate – you will not be able to complete the following steps successfully. Please insure you have path access to the Certificate from the computer you are presently working on.

To import a Certificate, perform the following steps:

1. **Start Microsoft Internet Explorer**

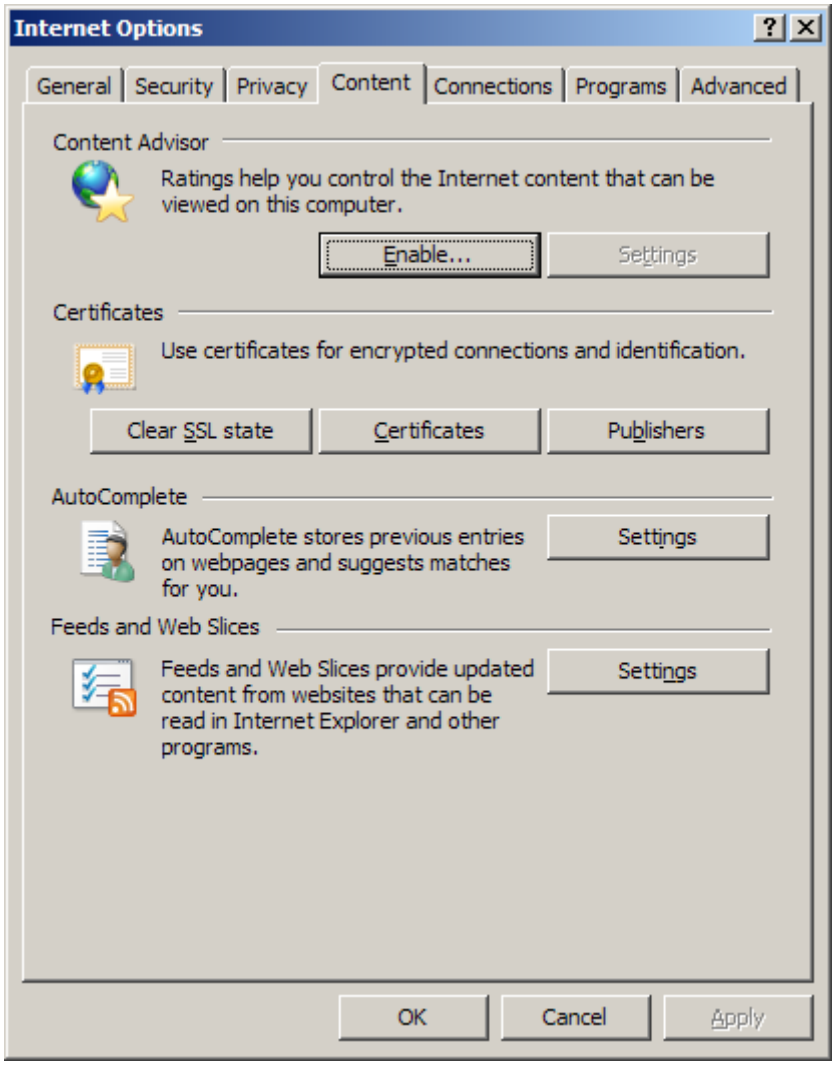
   Instructions continue on subsequent pages.

2. **Invoke Internet Options**
   On the IE toolbar will be an item called **Tools**. Clicking on **Tools** will invoke a menu where you will find an **Internet Options** item. Clicking the **Internet Options** item, which will invoke a window similar to the following (the window for IE 8 is shown below):



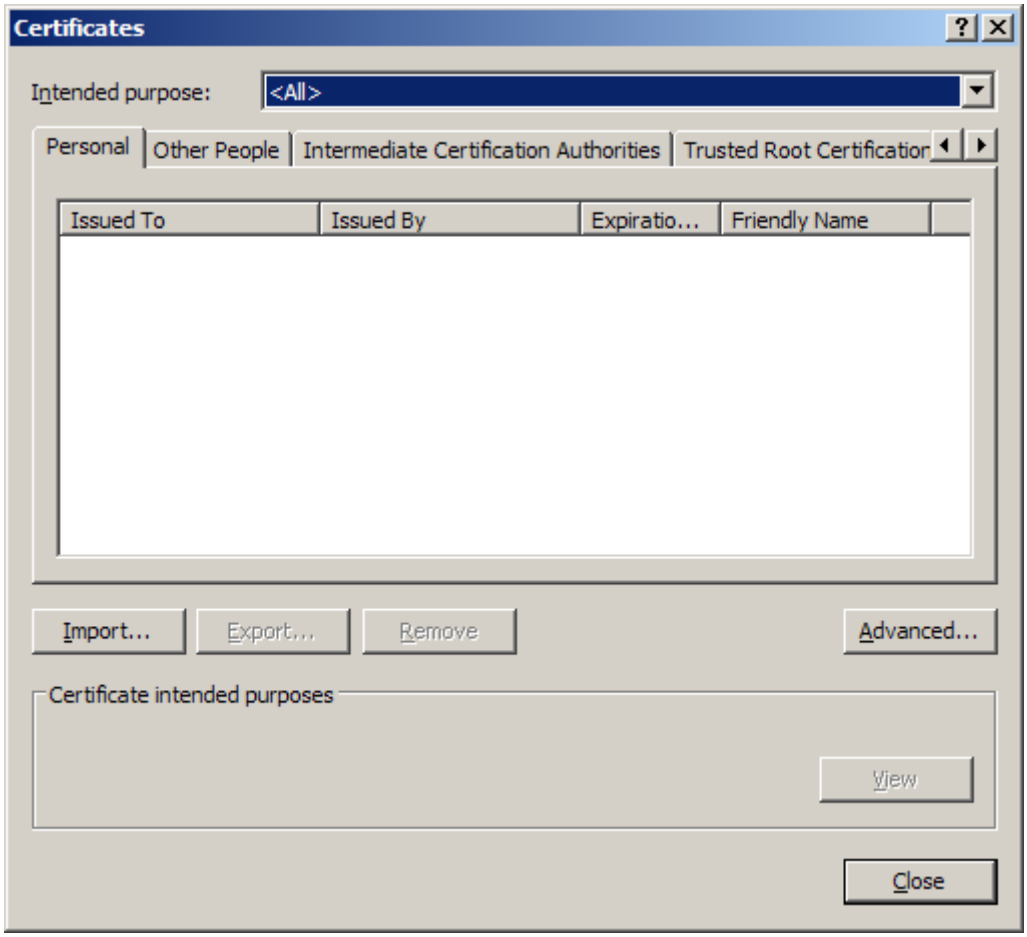
To continue, click on the Tab entitled **Content**.

3. **Internet Explorer, Content Tab**
   Clicking the **Content** Tab as described above will invoke the **Content** Tab, which will look similar to the following:



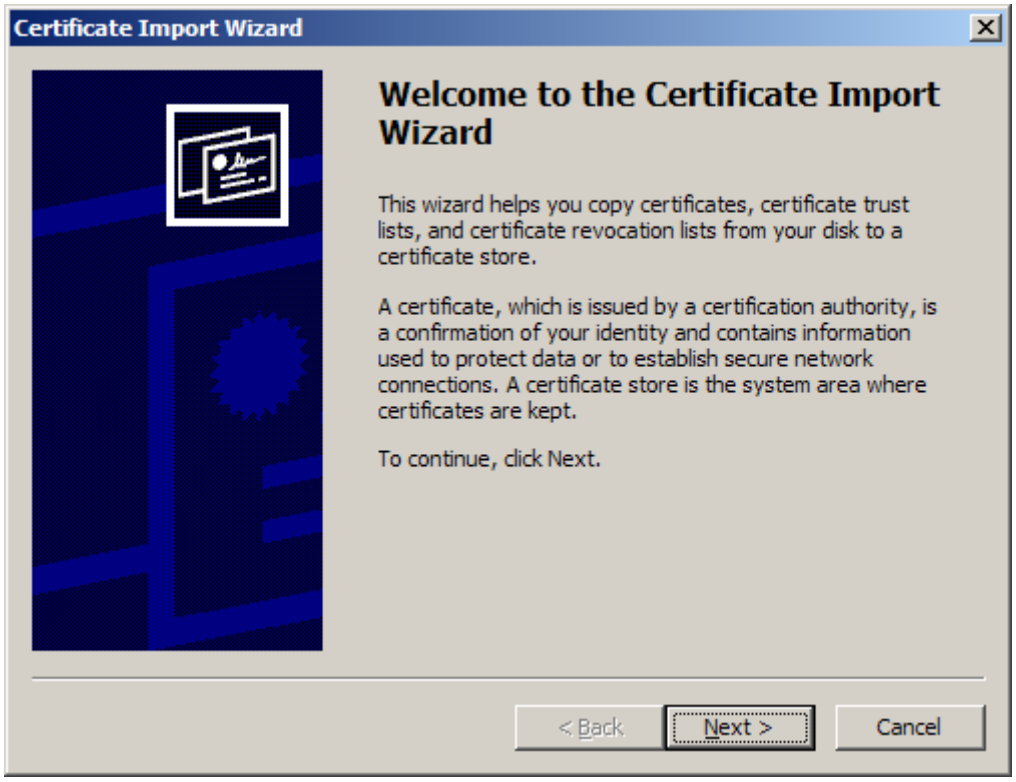
To continue, click the **Certificates** button located in the middle of the **Content** Tab. This will invoke a **Certificates** window.

4. **Internet Explorer – Certificates Windows**
   Clicking the Certificates button described above will invoke a window similar to the following:



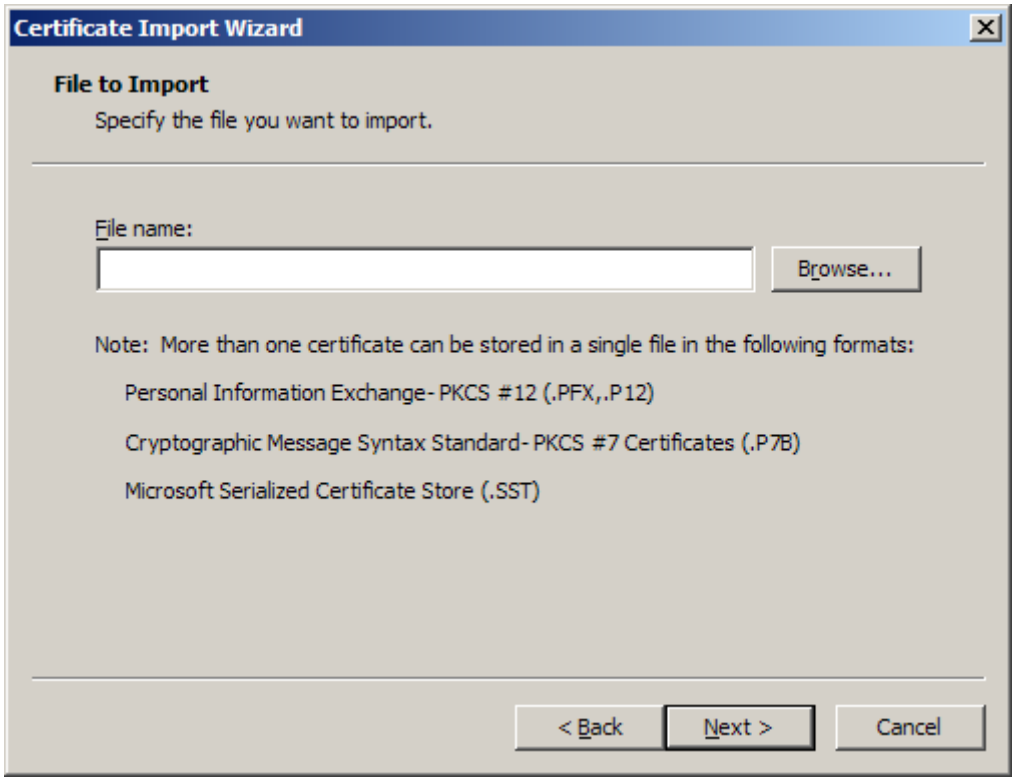
To continue, click the **Import** button on the **Certificates** window.

5. **Internet Explorer – Certificate Import Wizard – Step 1**
   Clicking the **Import** button as described above will invoke the first window of the **Certificate Import Wizard**, which will look similar to the following:



   To continue, click the **Next** button.

6. **Internet Explorer – Certificate Import Wizard – Step 2**
   Clicking the **Next** button as described above will bring up the next screen of the **Certificate Import Wizard**, which will look similar to the following:



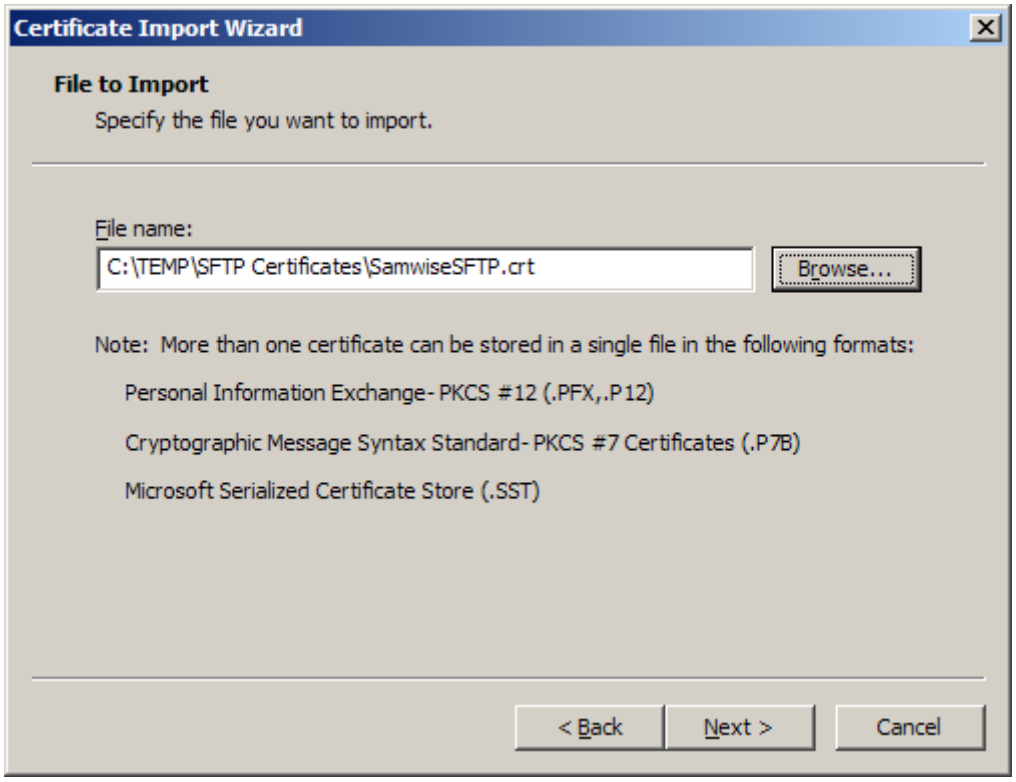
   To continue, click the **Browse** button.

7. **Internet Explorer – Certificate Import Wizard – Step 3**
   Clicking the **Browse** button as described above will invoke a typical Windows **Open** window that will allow you to navigate to the path where the Certificate that was provided to you has been temporarily stored.

   Navigate to the appropriate directory where the Certificate that was given to you has been saved, left-click on it to select / highlight this file.

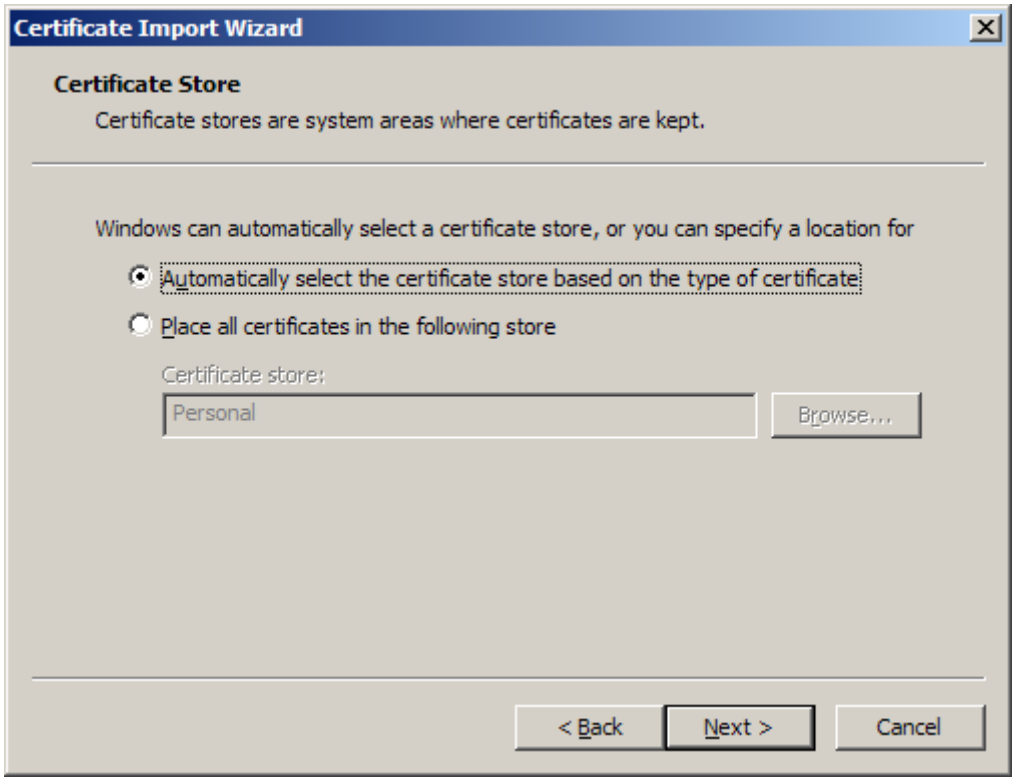
   To continue, then click the **Open** button.

8. **Internet Explorer – Certificate Import Wizard – Step 4**
   Performing the above action will return the user to the window seen in #6 above, with the appropriate Certificate file selected. This will now look similar to the following image:



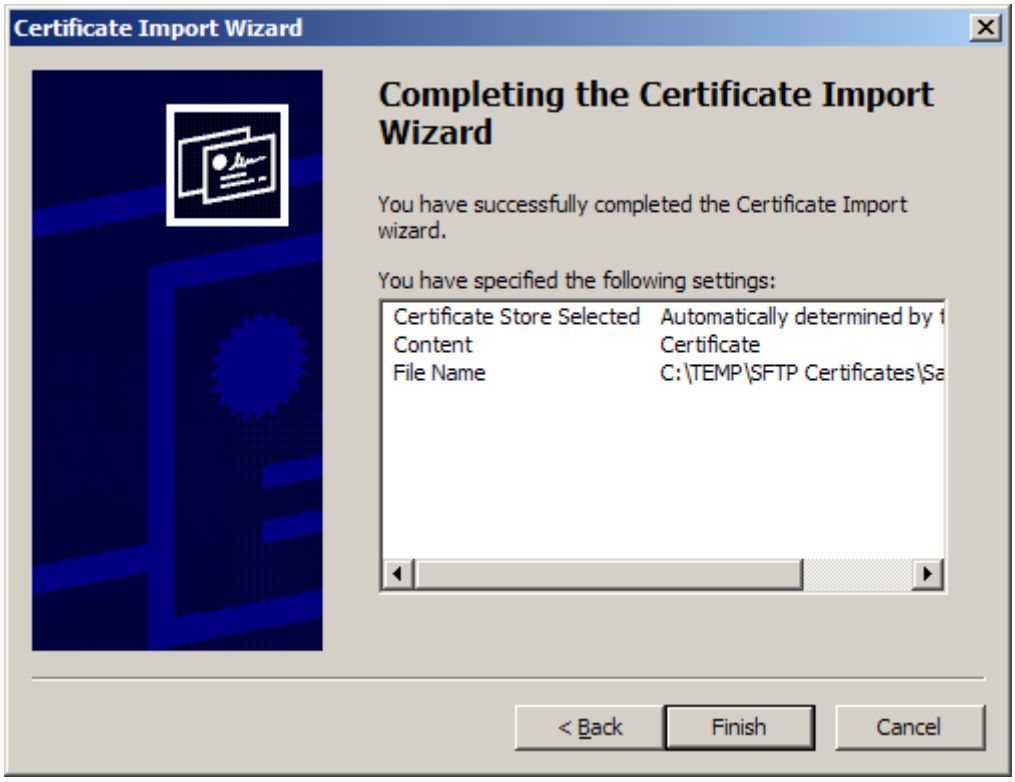
To continue, click the **Next** button.

9. **Internet Explorer – Certificate Import Wizard – Step 5**
   Performing the above action will invoke a window similar to the following:



To continue, first click the **Automatically select the certificate store based on the type of certificate** radio button (as shown above), then click the **Next** button.

10. **Internet Explorer – Certificate Import Wizard – Finish**
    Performing the above actions should now invoke a window similar to the following:



    To continue, click the **Finish** button, after which all remaining open IE windows may be closed as desired.

If the above steps were followed successfully, the appropriate Certificate should now be loaded into the Windows Certificate Store (which is located within the Windows Registry), and Secured FTP communications using NatQuery against the remote FTP platform may occur.