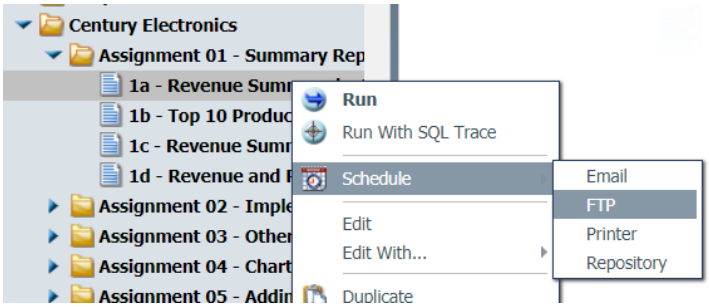
Distributing Db2 Web Query Reports using Secure FTP

The Report Broker tool in Db2 Web Query provides scheduling and distribution capabilities for reports. One of the distribution options is to transfer a report's output to a remote file on an FTP server. This technote provides information for creating a schedule and distributing its report output using the SSH File Transfer Protocol (SFTP), also known as the Secure File Transfer Protocol. Although SFTP clients have similar function as FTP clients, they use different protocols.

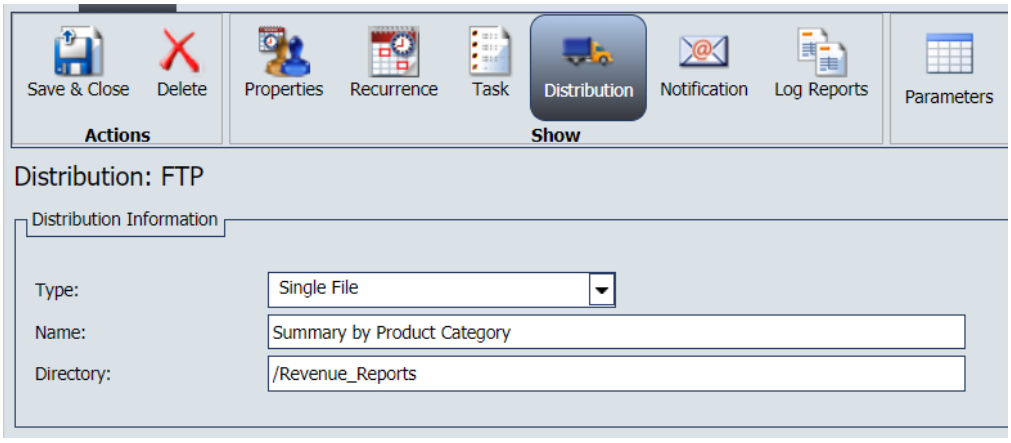
Scheduling a Report for FTP

Schedules are easily created as a right-click option for reports on the BI portal. To create a schedule and designate FTP distribution, sign into Web Query and perform these steps.

1. Right click the report. Select Schedule, and then select FTP.

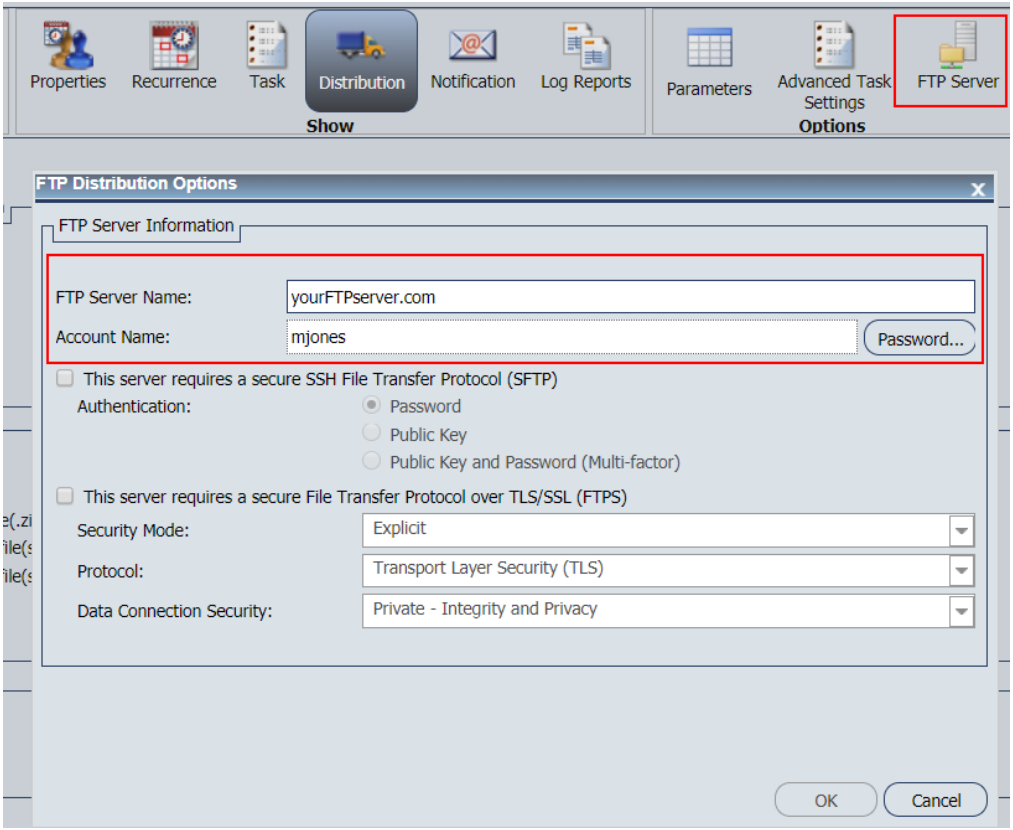


2. Click the Distribution icon on the ribbon. Select Single File for the Type. Enter the Name of the target file to receive the report. If the file doesn't exist, Report Broker will create it. Enter the Directory path for the target file. Report Broker will not create the directory.



3. Click the FTP Server icon on the ribbon. This launches the FTP Distribution Options panel. For traditional FTP, enter the FTP Server Name and an Account Name and Password that will be

used for logging into the FTP server. Click OK.



You can save the schedule as is or continue to customize it with recurrence intervals, parameters, notifications, and other properties. To change the schedule to use SFTP instead of traditional FTP, proceed to the following sections.

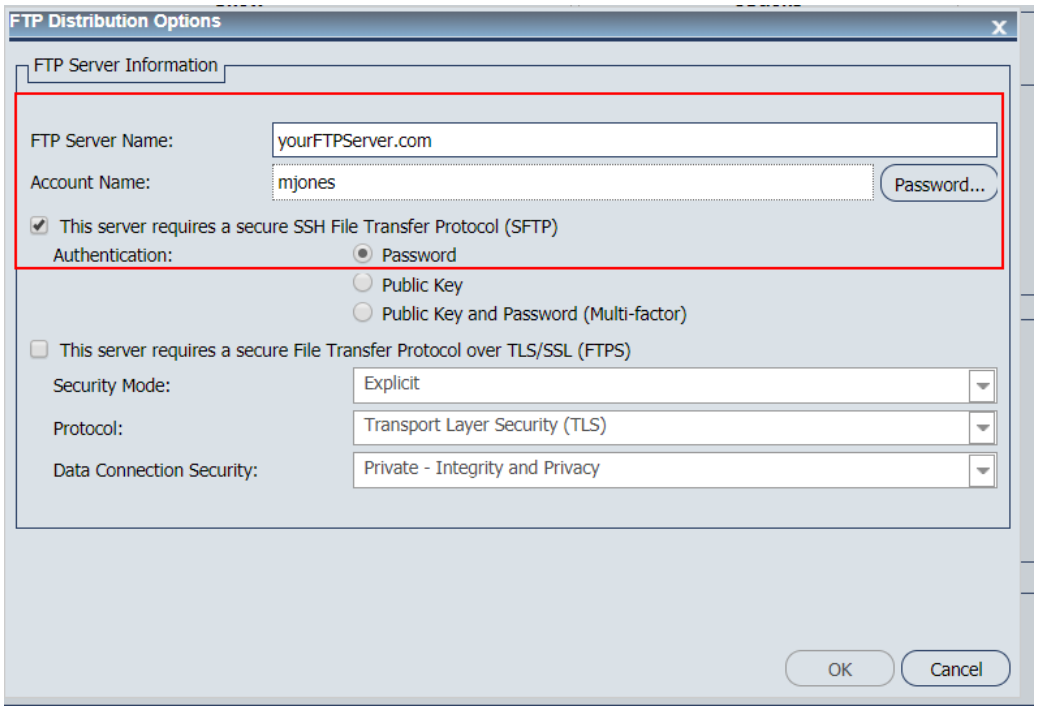
Setting SFTP Password Authentication

The Password authentication option uses a password to authenticate the user to an SFTP server. Make sure the Account Name you enter for the user exists on the FTP Server and that you specify a valid password. The Account Name applies to the FTP server and is independent of the execution/owner ID of the schedule.

To use SFTP password authentication, specify the FTP Server information as follows:

1. Enter the FTP Server Name, Account Name, and Password.
2. Click the box for SFTP.
3. Click Password.

4. Click OK.



5. Save the schedule.

Setting SFTP Public Key Authentication

The Public Key option enables use of an OpenSSH public/private key pair for enhanced security. The server proves its ID to the client. The client proves the user's ID to the server. Data is encrypted with a shared public key. It is decrypted with a non-shared private key.

The Web Query Distribution Server requires a copy of the private key. A restriction is that the Distribution Server can handle only one private key per Web Query installation. That means all schedules using Public Key authentication must specify the same FTP Server, Account Name, and password.

There are setup steps needed on the client, server, and within the schedule for Public Key authentication. The steps below provide guidance. They use an example FTP Server named *yourFTPserver* and an example Account Name *SFTPUSER*.

Step 1: Client-side Setup

1. Install prerequisite products. The following must be installed:
   - 5733SC1 *BASE - IBM Portable Utilities for i
   - 5733SC1 Option 1 – OpenSSH, OpenSSL, zlib
   - 57xxSS1 Option 33 - Portable Application Solutions Environment (PASE)
2. Create a user profile and home directory for the user specified on the Account Name. The default home directory for a user is /home/*userid*. You can change it to another directory, if you prefer,

using the CHGUSRPRF command. SSH stores files in the user's home directory under the .ssh subdirectory. Make sure the permissions are correct on the home directory, else it may be difficult to diagnose problems later. Following are commands to create the default home directory and grant the authorities.

a. `CALL QP2TERM`
b. `mkdir /home/sftpuser`
c. `chown sftpuser /home/sftpuser`
d. `chmod 755 /home/sftpuser`
e. Press F3 to exit QSH.
f. `CHGUSRPRF USRPRF(SFTPUSER) HOMEDIR('/HOME/SFTPUSER')`

3. Generate the public/private key pair. SSH supports more than one type of keys. The example keygen command below uses the default key type, rsa. Because the private key is afterall private, these steps should be performed by SFTPUSER.

g. `qsh`
h. `ssh-keygen -t rsa -P ''`
i. When prompted for the file name, press Enter to use the default.

The keygen command creates the /home/sftpuser/.ssh subdirectory and generates the public and private keys in .ssh. The names of the generated files are:

id_rsa --- This file contains the private key.
id_rsa.pub --- This file contains the public key.

4. Get the public key from the FTP Server. The below command retrieves the public key from the FTP Server and puts it in SFTPUSER's known_hosts file in .ssh. The key enables communications between the systems.

j. `Qsh`
k. `ssh-keyscan yourFTPserver.com >> ~/.ssh/known_hosts`

5. Sign out and sign back in with a profile that has *ALLOBJ and *SECADM authorities. Copy the private key to the Report Broker directory and grant authorities:

l.
```
CPY OBJ('/home/sftpuser/.ssh/id_rsa')
TODIR('/qibm/userdata/qwebqry/base8 0/reportcaster/cfg')
OWNER(*KEEP)
```
m.
```
RNM OBJ('/qibm/userdata/qwebqry/base80/ReportCaster/cfg/id_rsa')
newobj('sftp_private_key.txt')
```
Note: The sftp_private_key.txt file MUST have ASCII CCSID 819. You can confirm that the file is tagged with CCSID 819 using `wrklnk '/qibm/userdata/qwebqry/base80/ReportCaster/cfg/sftp_private_key.txt'` and selecting option 8. Confirm the contents are in CCSID 819 using wrklnk option 5 followed by F15.

n.
```
CHGOWN
OBJ('/qibm/userdata/qwebqry/base80/reportcaster/cfg/sftp_private_key
.txt') NEWOWN(QWQADMIN)
```
o.
```
CHGAUT
OBJ('/qibm/userdata/qwebqry/base80/reportcaster/cfg/sftp_private_key
.txt') USER(*PUBLIC) DTAAUT(*NONE)
```
p.
```
CHGAUT
OBJ('/qibm/userdata/qwebqry/base80/reportcaster/cfg/sftp_private_key
.txt') USER(SFTPUSER) DTAAUT(*RWX)
```

Step 2: Server-side Setup

Send the public key file, `id_rsa.pub`, to the FTP Server administrator via FTP or email. Use binary mode if you use FTP. The administrator will transfer the file to the FTP Server.

If the FTP Server is an IBM i, SSHD Server, public keys are stored in SFTPUSER's .ssh directory in the authorized_keys file. The server administrator should copy the file and set authorities as follows:

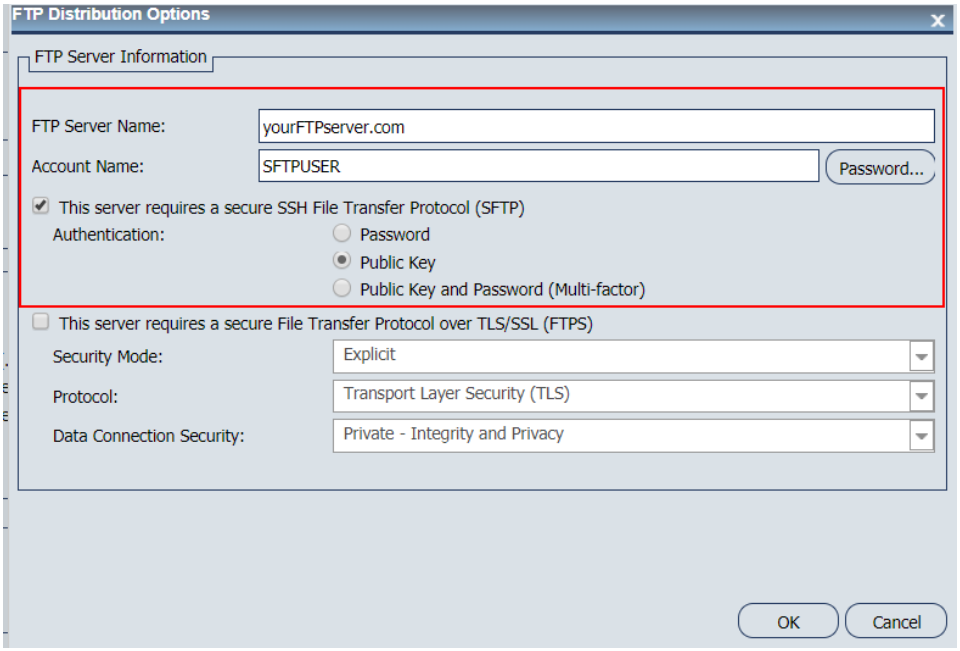
1. If the `authorized_keys` file does not already exist, FTP the `id_rsa.pub` file in binary mode to the .ssh directory and rename it to authorized_keys. If the `authorized_keys` file does already exist, then use the following example commands to append the key to the file, where /tmp is the path of the `id_rsa.pub` file and /home/sftpuser is the user's home directory.
   a. `qsh`
   b. `cat /tmp/id_rsa.pub >> /home/sftpuser/.ssh/authorized_keys`
2. `CHGOWN OBJ('/home/sftpuser/.ssh/authorized_keys') NEWOWN(SFTPUSER)`
3. `CHGAUT OBJ('/home/sftpuser/.ssh/authorized_keys') USER(*PUBLIC) DTAAUT(*NONE)`

Step 3: Schedule Setup

With SFTP, the Account Name and Password are needed for logging in to the FTP Server. The Public Key authentication adds the ability to encrypt communications between the Web Query Distribution Server and the SFTP server with the server logon still present. Simply said, you still need the Account Name and Password for Public Key authentication.

To complete the schedule, do the following.

1. Enter the FTP Server Name, Account Name, and Password.
2. Check the box for SFTP.
3. Click Public Key.
4. Click OK.
5. Save the schedule.



You are now ready to run the schedule and test the SFTP transfer.

References:

- Refer to this link if you'd like to configure an IBM i SSHD Server to Use Public-Key Authentication **http://www-01.ibm.com/support/docview.wss?uid=nas8N1012709.**