This document provides an example of using a Dynamic Distribution List to password encrypt Report Broker output. You can encrypt both email attachments and FTP files, but they must be *zipped* because Web Query uses the password encryption feature of zip in its implementation.

For the following example commands, we will send a password protected report to multiple email destinations. The email addresses and passwords are stored in a Db2 table. Note that a production application might dynamically generate and encrypt the passwords.   For more information on Dynamic Distribution Lists, refer to the New Features 2.1.0 document at http://ibm.biz/db2wq-newfeats. To encrypt the passwords, a suggestion is to use the Db2 SQL function ENCRYPT_AES or ENCRYPT_TDES.

Part 1 – Create a data source for your destination email addresses and passwords. You can assign a separate password to each recipient if you like. The email address field should be 50 characters and the password field should be 10 characters.

1. create table qgpl/dynamic_dist_list   (dest char(50) not null, pass char(10) not null)
2. rename qgpl/dynamic_dist_list to system name dyndislist
3. insert into qgpl/dyndislist values('abc@somewhere.com', 'passw0rd')
   insert into qgpl/dyndislist values('xyz@somewhere.com', 'passw1rd')

Part 2 - Create a stored procedure that builds the dynamic distribution list that is passed into Report Broker.

4. create procedure qgpl/get_dist_list( )
   result sets 1
   language sql
   specific dyndislist
   p1: begin
       declare c1 cursor with return for
       select dest, pass from qgpl.dynamic_dist_list;
   open c1;
   end p1
5. chgobjown qgpl/dyndislist objtype(*file) newown(qwqadmin)
6. chgobjown qgpl/dyndislist objtype(*pgm) newown(qwqadmin)

Part 3 - Update the dynlist.fex that is shipped with Web Query to add in the password (PASS) parameter. (Note: another approach would be to copy dynlist.fex into a new dynpass.fex and update that instead.)

7. wrklnk '/qibm/userdata/qwebqry/apps/baseapp/dynlist.fex'
8. Select option 2 to edit the file. Add the password (PASS) parameter after DEST as shown in the screen shot below.

9. Press F3 to Save your changes.

Part 4 - Create and run your schedule.
10. Sign on the Web Query portal at https://<system>:12331/webquery. Right click your report and select Schedule-> Email.
11. Click Distribution on the ribbon and fill in the form. For Type, select Dynamic Distribution List. This enables the 'To' parameter where you click the ellipse and enter the dynlist fex and its SQL stored procedure parameter as such: DYNLIST SQLPROC=qgpl/dyndislist. Click OK.

Dynamic Distribution List from Server Procedure ✕

Server Name:	EDASERVE ▼
Execution ID:	mnw ▼
Procedure Name:	DYNLIST SQLPROC=qgpl.dyndislist Browse...

OK   Cancel

12. Enter a Reply Address and Subject. Lastly, be sure to click the 'Add Report to Zip File' checkbox and enter a Zip File Name. See the screen shot below for our example flow.

13. Click Email Server on the ribbon and enter your Mail Server Name.
14. Click Save & Close, and assign a name to your schedule.
15. You should now see your schedule on the portal tree. Right click and Run it.
16. Verify the schedule ran successfully. Right click on the schedule and select View Log, then click OK. Check for errors in red text.

Part 5 – Viewing the protected report.

17. To view the report, your recipients will first need to unzip it and provide their password. Use 7zip, winzip, or some other zip utility that supports the password encryption to extract the file. (Note that Windows Explorer will unzip it but does not support the password so you will get an error if you use it.) The recipient will be prompted to enter their password before the file is unzipped.