COGNOS8 SECURITY

This document describes the differing levels of security available for set up in Framework Manager, Report Studio and Cognos Connection

1 SUMMARY

There are three methods of setting up dynamic security, all of which are done in Framework Manager. These are discussed within this document along with examples. This document does not discuss portal security relating to package, object and capability access.

Digital Viper Limited takes no responsibility for the accuracy or the use of this document.

2 ROW LEVEL / DATA LEVEL SECURITY

This is the simplest form of security and is achieved by using a fixed filter for each user class or group of user classes.
1. Select the query subject - right click and select 'Specify security filters'
2. Click the 'Add Groups' button.
3. Select the user classes you require from the LDAP/AD/NTLM namespace. (For example 'Japan users')
4. Click in the box below 'Filter' and select 'Create/Edit Embedded'. This will open a filter definition window.
5. Enter a filter definition and click OK. For example Country_Code ='JP'
6. Click OK again to exit the set up window.

The security filter will become active once the package the query subject belongs to is published. At runtime when any users with the applicable user class uses a report based on the query subject the query results will be filtered using the filter definition you specified. (In my example all user in the user class 'Japan users' will only have the ability to view data with a country code of 'JP').

Rather than setting up this security many times, try to set it up on a common or conformed dimension query subject.

3 DYNAMIC FILTERING (CSVIDENTITYNAMELIST)

This security set up is similar to the first option but is more dynamic in that the filter definition does not have to be altered every time the user class structure is changed. This option is also useful where a large number of user classes are used.

The security method can be used against table held entries or against a calculated query item and matches the user class in the LDAP to an entry in the table (or query item).

1. Select the model query subject that you wish to set up the security on.
2. Right click and select 'Edit definition'
3. Click on the filter button/tab (to add a new filter)
4. Add the required query item to the filter expression.
5. Add the CSVIdentify function to the expression. The end result should look like the following sample:

```
([Presentation Layer].[Countries].[Country_Code] in (#CSVIdentityNameList()# ))
```

6. Add any additional filters using a 'OR' to ensure that Administrators and report developers are not filtered:

```
('Administrators' in (#CSVIdentityNameList()# ))
OR
('Report Administrators') in (#CSVIdentityNameList()# ))
OR
([Business Layer].[Countries].[Country_Code] in (#CSVIdentityNameList()# ))
```

7.Click OK twice to enable the filter.

The security filter will become active once the package the query subject belongs to is published. At runtime the filter will activate when the query subject is used. The filter works because the CSVIdentifyNameList function lists all userclasses that the runtime user is a member of and then filters against the calculation or table entry. Again - this method is best used where large volumes of user classes are used such as account numbers.

4 BURST RECIPIENT (CAM ID)

This method of security only hides burst report output within Cognos connection but it is useful when users of many different classes access the same folder to view report output. It should be noted that user should only have read, traverse access to the folder. The report burst should be done by a more senior account such as directory admin or report admin.

1. Within Framework Manager add a calculated query item to the query subject that either contains a list of the user classes or where the user class can be calculated.
2. Use a static case statement to define the calculation (an example is shown below):

```
CASE ([Business Layer].[Countries].[Country_Code] )
WHEN 'JP' THEN ('CAMID("EP Series7:r:authid=3771403238")')
WHEN 'MA' THEN ('CAMID("EP Series7:r:authid=3771403548")')
WHEN 'NL' THEN ('CAMID("EP Series7:r:authid=3049983260")')
WHEN 'NZ' THEN ('CAMID("EP Series7:r:authid=197856540")')
WHEN 'PO' THEN ('CAMID("EP Series7:r:authid=2680884508")')
WHEN 'RO' THEN ('CAMID("EP Series7:r:authid=3872066844")')
WHEN 'SE' THEN ('CAMID("EP Series7:r:authid=4123725084")')
WHEN 'SI' THEN ('CAMID("EP Series7:r:authid=13307164")')
WHEN 'ZA' THEN ('CAMID("EP Series7:r:authid=2999651612")')
ELSE (NULL)
END
```

3. Use the recipient user class CAM ID as the CASE statement result for the user class or calculation. (This can be found in Cognos Connection by selecting the properties of the user class from the directory.)
4. Publish the package that includes the altered query subject.
5. Within the report add the new query item that uses the CASE statement.
6. Change the burst options of the report so that the burst recipient is based upon the new query item. (The report should be burst so that the report output is logically linked to the userclass selected ie. Japan users can only see the Japan result of the burst report). Make sure that the report bursts to a directory entry.
7. Run the report and burst it.

As the administrator/directory administrator you should be able to check that the report burst correctly and that all report outputs have been created.
Check the security filter works by logging in to Cognos Connection as a user with access to a userclass listed in the CASE statement. When you select show multiple outputs you should only see the output pertaining to the user class.

COPYRIGHT AND USE

Please feel free to use the ideas and methods discussed in this white paper. All we ask in return that you add a link to www.digitalviper.co.uk to your website and /or documentation. You may even wish to book our time to set the system up for you.

The 4 bars image is a trademark of Digital Viper and may not be used without express written permission.