Proven Practice

Security in Framework Manager

Product(s): Framework Manager

Area of Interest: Security
Copyright

Copyright © 2008 Cognos ULC (formerly Cognos Incorporated). Cognos ULC is an IBM Company. While every attempt has been made to ensure that the information in this document is accurate and complete, some typographical errors or technical inaccuracies may exist. Cognos does not accept responsibility for any kind of loss resulting from the use of information contained in this document. This document shows the publication date. The information contained in this document is subject to change without notice. Any improvements or changes to the information contained in this document will be documented in subsequent editions. This document contains proprietary information of Cognos. All rights are reserved. No part of this document may be copied, photocopied, reproduced, stored in a retrieval system, transmitted in any form or by any means, or translated into another language without the prior written consent of Cognos. Cognos and the Cognos logo are trademarks of Cognos ULC (formerly Cognos Incorporated) in the United States and/or other countries. IBM and the IBM logo are trademarks of International Business Machines Corporation in the United States, or other countries, or both. All other names are trademarks or registered trademarks of their respective companies. Information about Cognos products can be found at www.cognos.com

This document is maintained by the Best Practices, Product and Technology team. You can send comments, suggestions, and additions to cscogpp@ca.ibm.com.
## Contents

1. **INTRODUCTION** ................................................................. 4
2. **PACKAGE SECURITY** .......................................................... 4
3. **OBJECT SECURITY** ............................................................. 6
4. **DATA SECURITY** ............................................................... 10
1 Introduction

When dealing with security in IBM Cognos 8 we are referring to the external 3\textsuperscript{rd} party security that you may be using. This does not include the Cognos Namespace which contains the groups and roles that we have created for you if you choose to use them. The use of the pre-created groups and roles is not necessary.

When implementing security in Framework Manager a user has the ability to control access to an object, package or data.

2 Package Security

There are two places where package security can be implemented, in the package wizard when initially creating the package (figure 1), and in IBM Cognos Connection in the “Set Properties” section of the Action Menu (figure 2).

Figure 1.
The security you set will control the ability to use the package in one of the IBM Cognos 8 Studios, as well as the ability to run a report that uses that package. A user with restricted access to a package will be able to see any saved output in a report that has been already run.

It's also possible to specify a list of users or roles which have administrative access to the package (figure 3). Administrative access you are granting permissions to republish the package as well as perform an impact analysis on the package to determine which reports will be impacted by the changes made.
Figure 3.

3 Object Security

It is possible to restrict access to specific objects in a project, for example if you have a user or group of users who you don’t want access to a particular Namespace then you can remove access to that Namespace for that user or group of users. Objects which can have security applied include namespaces, query subjects, query items, filters and folders. You can either Allow (make visible) or Deny (not visible) access to these objects (figure 6).
You must ensure when granting access to an object that the user or group of users you are granting access to, also have access to the package that contains them. When running a report in which a user or group of users does not have access to one or more objects in the report (i.e., a query item, or query subject) then the report will fail (figure 7), however a user can still view saved reports outputs even if they don’t have access to one or more of the objects in the saved report.
By default the everyone group is on the access control list for every object in a project, and if you add a user, group or role to an object then it will be added to the access control list of every object in your project. Any new object that is created will inherit the permissions of its parent object in the project. Permissions must be explicitly granted for users, groups or roles, so if you grant access to an object for a particular user in a project that user is automatically added to the ACL (access control list) for every object in the project and all other users, groups, or roles will automatically be denied access to all other object until permission is explicitly granted.

It is also possible that a user is a member of more than one group, and the groups have conflicting access to an object. For instance the group1 group is granted access to an object, whereas the group2 group is denied access to the same object (figure 8a & figure 8b). The end result is the user is DENIED access to that object (figure 9). Denied access always overrides the granted access when dealing with Object Security.
Figure 8a.

Figure 8b.
There are two concepts when performing Object Security in Framework Manager. You can either Deny access to everyone for everything in the project, then explicitly grant access for the users that need access to each object. Or you can Allow everyone access to everything in the project and then deny access to those users you wish to restrict. Denying access to everyone for everything is a simply matter of specifying object security to any object at any level for one particular user or group. By default all other users or groups will be denied access to everything else in the project. Granting access to everyone is a simple matter of granting Allow access to the root namespace for the Everyone group. By default everyone will now have access to everything in the project and you can now Deny permissions for specific users, groups or roles as need be.

4 Data Security

It’s also possible to restrict part or all of the data that a particular Query Subject returns to a user or group of users by applying a security filter on the Query Subject in Framework Manager. The security filter can make use of macros or parameter maps to further enhance the abilities of the filter. If a user or group is not listed in the security filter then that user or group has unrestricted access to that query subject. You can specify data security by highlighting the object you wish to filter and then select “Specify Data Security” from the Actions menu. In the window that opens you can select the groups or users you wish to filter and either create a new filter or use an existing filter condition to apply to the user or group (figure 4.)
After publishing the package now when a user or a role defined in the Data Security window runs a report they are only permitted to see the data for which the filter applies. For example if Joe logged into Query studio and created a report with Issue_Type and Issue_Date he only will only see the issue types which are greater than 2 (figure 5).