DOQ Catalogue

# Must be secure!

The way DOQ operates it allows for a constant connection with the server. In order to keep everyone who communicates with DOQ from access every part of the database, a security modal was created.

# Terms

The terms used in the security filter file are as follows:

* User: A user is a connection to DOQ that has been accepted, and allows queries.
* Group: A group is a set of security rules applied across multiple users. Many groups can be assigned to each user.
* Act Level(Action Level): Represented by an octal decimal number, it is the assignment of how much access is allowed on a database node. 1 – Execute, 2 – Write, 4 – Read.
* Database Node: The connection node, and any node within the connection, which can include a table, a column, and object data within a column that has been turned into an object.
* Base act: The access that everyone is given.

# Usage

One part of the security is a catalogue xml file, for a full reference of all the elements in the file See Structure of the catalogue XML in this file. Each connection store should have a throughout catalogue for security, as well as to take advantage of the caching mechanisms.

The base level for everyone accessing the store is stored in the ‘connections’ node, which contains all the connection catalogues for the store. The flow of the security works as the last listed, so if ‘/node’ has read and execute but ‘/node/node’ has only execute then the last update to the security takes over. In the case of users it is the same, if the user has no updates then there permission is as listed prior. The groups, and exact user information is optional. Any user with a username or group not stored in the catalogue will be considered as if permissions under all users/groups didn’t apply. As a way to prevent break in, maxAnonymousQueries can be setup to notify an administration of ran queries, as well as block further queries by a length of time in hours defined by lockOutTime. These node attributes are optional for every ‘connection’ and ‘node’.

## Catalogue

The main node must be name catalogue.

* Atb:**admins** – A comma delineated list of e-mails for administers to be notified of suspicious behavior. This attribute is optional, and regardless of it activity can be logged.
* Atb:**logLevel** – How detailed of a log to keep, options are none, secure, query, and verbose. A secure log level only logs anonymous queries. A query log will log every single query. While a verbose log will log every query as well as every result sent back successfully.  
  **Default** is secure.
* Node:**groups** – See Groups.
* Node:**users** – See Users.
* Node:**connections** – See Connections.

## Groups

The node that contains all the group nodes for the catalogue.

* Node:group – See Group.
* Atb:**defaultAccess** – What every group should by default be for every node in the catalogue.  
  **Default** is off.

## Group

A group for the catalogue.

* Atb:**id** – The id of the group.
* Atb:**baseAct** – The base act level for any user in the group.
* Atb:**defaultAccess** – What the group should be by default for every node in the catalogue.  
  **Default** is inherited.

## Users

The node that contains all the user nodes for the catalogue.

* Node:user – See User.
* Atb:**defaultAccess** – What every user should by default be for every node in the catalogue.  
  **Default** is off.

## User

A user for the catalogue.

* Atb:**id** – The id of the user.
* Atb:**baseAct** – The base act level for the user.
* Atb:**defaultAccess** – What the user should be by default for every node in the catalogue.  
  **Default** is inherited.
* Atb:**groups** – A coma delineated list of groups the user is affiliated with.

## Connections

The node that contains all the connection nodes for the catalogue.

* Atb:**baseAct** – The base act level for anyone using this catalogue. **Default** is 01.
* Atb:**allowAnonymous** – Identifies if anonymous queries should be allowed in this catalogue. Value can be set to ‘true’ or ‘yes’  
  **Default** is ‘false’
* Atb:**maxAnonymousQueries** – The maximum number of queries a non-user can perform. The number zero being unlimited.  
  **Default** is 25.
* Atb:**maxAttemptedQueries** – The maximum number of queries a user can perform where there permission is denied. The number zero being unlimited.
* Atb:**lockOutTime** – The amount of time in hours to lockout a user when they hit the maximum number of queries both anonymous, and disallowed. The number 0 being until the lock out is removed by administration from the lock out file.  
  **Default** is 24 which is one day.
* Atb:**defaultFilter** – The default filter that is applied to nodes that have no filter.
* Node:**connection** – See Connection

## Connection

A connection for the catalogue to allow queries.

* Atb:**id** – The id of the connection.
* Atb:**baseAct** – The base action for the connection if different then the connections node baseAct.  
  **Default** is inherited.
* Atb:**groupAct** – A comma list of groups that have different permission from there base permissions. For all use \*.
* Atb:**userAct** – A comma list of users that have different permissions from there base permissions. For all use \*.
* Atb:**allowAnonymous** – See Connections/allowAnonymous.  
  **Default** is inherited.
* Atb:**maxAnonymousQueries** – See Connections/allowAnonymous.  
  **Default** is inherited.
* Atb:**maxAttemptedQueries** See Connections/maxAttemptedQueries.  
  **Default** is inherited.
* Atb:**lockOutTime** – See Connections/lockOutTime.  
  **Default** is inherited.
* Node:**node** – See Node.

## Node

A node for the connection

* Atb:**indexBy** – As a way to speed up the get and push to database a cache mechanism uses indexBy to index a set of node entries, and keeps them in the memory. A node that does not have an indexBy will not be cached at all.
* Atb:**id** – The id of the node.
* Atb:**baseAct** – The base action for the node if different then the connection node baseAct. **Default** is inherited.
* Atb:**groupAct** – See connection/@groupAct.  
  **Default** is inherited.
* Atb:**userAct** – See connection/@userAct.  
  **Default** is inherited.
* Atb:**allowAnonymous** – See connections/@allowAnonymous.  
  **Default** is inherited.
* Atb:**maxAnonymousQueries** – See connections/@allowAnonymous.  
  **Default** is inherited.
* Atb:**maxAttemptedQueries** - See connections/@maxAttemptedQueries.  
  **Default** is inherited.
* Atb:**lockOutTime** – See connections/@lockOutTime. **Default** is inherited.
* Atb:**filter** – The filter used to understand the node.  
  **Default** is inherited from connections/@defaultFilter.
* Node:**node** – See Node.