Cognos Security Policy

A look at the security policy that is in place for the ODS/Cognos Reporting Environment at the College of Charleston

Mary L. Person
11/13/2012
Table of Contents

Overview .................................................................................................................................................. 2
Initiating a Request for an account .......................................................................................................... 3
Levels of Security .................................................................................................................................... 4
   ODS Oracle Account ................................................................................................................................. 4
   ODS Oracle Roles .................................................................................................................................. 4
   Active Directory ...................................................................................................................................... 5
      Active Directory Account ....................................................................................................................... 5
      Cognos Security Groups ....................................................................................................................... 5
   Other Active Directory Groups ............................................................................................................... 6
   Cognos Connection ................................................................................................................................. 7
      Tying the AD account to the ODS Oracle ID ..................................................................................... 7
   Permissions on Folders ............................................................................................................................. 7
   Permissions on Packages ........................................................................................................................... 8
   Data Specific Security ............................................................................................................................... 9
      Data Owners and AD Data Security Groups .................................................................................... 9
      Social Security Numbers .................................................................................................................... 9
Sharing Data or Reports ............................................................................................................................ 10
Overview

Data Security within the reporting environment of the Operational Data Store (ODS) and Cognos has many layers. To access data, a person must have an Oracle ID on the Production or Test ODS database, an Active Directory account in one or more of the Cognos security groups, an Active Directory account in one or more of the Cognos data/tools groups, and a link between the two accounts. To get all three of these, a user must additionally attend training offered monthly by the Information Management Office within Institutional Research and Planning (IRP). Multiple groups within IRP, IT and data owners’ offices participate in applying the various pieces of the policy, but it is all initiated by a request by either the data owner’s office or the end user. This document will cover initiating a request for a user account, the levels of security that exist, the steps for implementation for a user, and what is taught in training to users regarding security.

The various levels of security ensure that College of Charleston’s Cognos users have a variety of permissions allowed. The CognosDataAccess_OU Active Directory group gives users in Cognos with explicitly granted permission to access each type of data on which their job rely. The CognosRoles_OU and CognosDataAccess_OU combination also ensures that an end user is able to run reports or publish reports based on the approved and granted access. Other Active Directory groups are used to give users permission to reports that have been published and need to be secured to particular fields within reports. An ODS Oracle Account ensures that the permissions granted in Banner are the same permissions granted in Cognos and the ODS. Folder and Package permission with Cognos ensure a second level of security for the users’ data type permissions.
Initiating a Request for an account

Written approval must be in place for a user to have access to each type of data. The first step in getting access through Cognos is achieved through one of two methods: the data owners submit the forms through the College’s new employee data security business process or an end user submits a Cognos license request.
Levels of Security

ODS Oracle Account

**Responsible party: Database Administrators**
A user must first have an Oracle ID set up on the Operational Data Store. Users access data on the database on an individual basis. As each person logs in to Cognos, that log in is tied directly to one Oracle account on the ODS database. The ODS Oracle account ensures that the person logging in to Cognos is accessing data to which that person has been specifically granted access.

**ODS Oracle Roles**

**Responsible party: Database Administrators**
An Oracle Role, in this case, is a group of tables associated with a specific type of data. The roles that exist are for Student, Finance Financial Aid, Accounts Receivable, Human Resources and Advancement.

All users are granted access to the Common role. This includes generic data such as name and address.

In order to be granted a role, the various Data Owners must explicitly grant in writing access to their data for a specified user. This permission comes from the Cognos license request approval or from the Security Office within IT passing on the approval from the data owner.
Active Directory
There are four levels of security which are tied to Active Directory (AD) within the ODS/Cognos reporting environment. The first is the user must have an Active Directory account. The second is the user must be included in the Cognos AD security groups. The third is Cognos report folders utilize existing security groups from AD to allow access to reports contained within those folders. The fourth is the user must be a member of an AD data specific security group in order to access data in those respective areas.

Active Directory Account

Responsible party: Identity and Access Management
Cognos users log in to the application using their College appointed username/password. Any College user can log in to Cognos, but only those included in one or more of the Cognos Active Directory groups are able to access anything.

Cognos Security Groups

Responsible party: Information Management
Within Active Directory is a CognosGroups_OU folder. Users must have their account added to at least one group from each of the Cognos Security groups. This determines what the user can do while in Cognos and to which data the user will have access. Within the main CognosGroups_OU folder are two subfolders which define the access as specified in the previous sentence.

CognosRoles_OU
These AD groups determine if a user is an author (writes or runs reports) or consumer (only runs reports). This includes four groups. The Analysis Studio, Query Studio and Report Studio groups allow a user to be an author and grants them access to those specific tools. A user in Report Studio or Analysis Studio has trickle down permission to use Query Studio, as well. Analysis Studio grants users permission to write reports against the Enterprise Data Warehouse (EDW), while the Report Studio grants users permissions to write reports against the ODS. The Consumer group allows users to run or schedule already published reports.

Snapshot of the CognosRoles_OU options
**CognosDataAccess_OU**

These groups determine if a user is an author or consumer for a specific data area. We use the CognosDataAccess_OU to determine to which data a user has access, as well as what the user can do with that data either consume or develop a report. A user can hold different roles within different data areas. For example, a user might be a Finance Author, but a Student Consumer. This may be true for a person who works in the Finance Office but needs access to some Student data.

![Snapshot of the CognosDataAccess_OU options](image)

**Other Active Directory Groups**

Responsible party: Information Management and various end users

Active Directory has many functional and security group set up within its structure. Most departments have a group created for them individually, and there are many subgroups and groups that encompass more than one Department, as well. These groups are used within Cognos to assign permissions to specific folders which contain reports relevant to that Active Directory Group. Please see the Permissions on Folders section of this document for further details about roles. These groups are also used to implement security for the medical/disability information and race/ethnicity data. Please see the Data Specific Security section of this document for further details about the data security specific to these two important areas.
Cognos Connection

Within the Cognos Connection interface, there is additional security. It includes tying the AD account to the previously described ODS Oracle ID and setting up permissions on folders and on packages. If a user attempts to log in and has not been set up by Information Management in any of the Cognos Security Groups he will not see folders or packages or be able to run any reports.

Tying the AD account to the ODS Oracle ID

Responsible party: Information Services

Each user has an individual Active Directory account, created by IAM, and an ODS Oracle ID, created by the DBAs. When a user logs in to Cognos, she uses her AD account and password. When she runs a report, Cognos looks to the Configuration to determine which ODS Oracle ID to use in order to return the appropriate data. By using individual ODS Oracle IDs, the College ensures that the data being returned are the data to which the specific user has been granted access. Via the Oracle Roles, FGA are implemented at this time. This is a manual procedure set up for each Cognos user by Information Services.

This feature ensures specifically that when two users click on the same Finance or HR report, they will return only data to which each has been granted access by the Finance Security Administrator. So if User A from Admissions runs a finance report, only the Admissions data to which that user has been granted access is returned. If User B from the Physical Plant runs the same report, only the Physical Plant data to which that user has been granted access is returned.

This is an extremely beneficial feature that the College chose to implement above and beyond the Ellucian recommended practice. It is high on maintenance, but the College’s data security is enforced at the column and row level.

Permissions on Folders

Responsible party: Information Management

The Cognos Connection has yellow folders which contain published reports that are available for Cognos users to run. Based on the data security granted by the Data Owners, the folders are secured using AD groups.

High level report folders are secured using the Cognos security groups within the CognosDataAccess_OU folder. (For more information on the CognosDataAccess_OU group, please see the Cognos Security Groups section of this document.) This level includes folders such as the generic “Finance”, “Student”, “Human Resources”, etc.

Within each of those main subject folders are a variety of subfolders. The Student folder, for example, includes 25 subfolders. Each of these are locked down separately according to the Registrar’s Office instructions. Absence Memo is a folder. The security for this folder includes the AbsenceMemo user and STAFabsences group, as well. No other users have access to see this folder, including the Registrar’s
Office users. *Academic Administration Reporting* is the primary folder for Student end user reports. There are 18 groups, such as Graduate Studies, Undergraduate Program Directors, Institutional Research, Academic Admins, Chairs and Deans, who have access to this folder.

If a user is not in one of the groups with approved access, he does not see the folder. If he should be in a group, the Registrar’s Office (RO) is notified and they initiate a request to the owner of the group to add the user to the group. Until that person is entered into the appropriate group, he does not see the folder and cannot run any reports for himself that are contained in that folder. Since the Registrar owns the data contained within the report, the RO can opt to run the report for him and share the results until his access has been set up properly.

All area’s subfolders work the same way. If someone does not have access to a folder but should, the request goes to the owner of the group to add them to the appropriate AD group or to Information Services to add them to the appropriate CognosDataAccess_OU group.

**Permissions on Packages**

**Responsible party: Information Services**

Packages are the blue folders seen in the Cognos interface. They are used by report authors to write the reports. Report consumers have no use for them functionally, but need to have access granted so the reports they are running will work properly. Permissions on packages are granted by Information Services using the AD groups within CognosDataAccess_OU and align with the Data Owners’ requests. The *Student Detail* package, for example, will be set up for a Student Author to have Read, Execute and Traverse permissions, while a Student Consumer will only have Execute and Traverse permissions. Some packages may overlap groups, so the *Active Registration* package has Student, Financial Aid, Admissions and Accounts Receivable author and consumer permissions set up.
Data Specific Security

Responsible party: DBAs and various end users
There are three elements of campus data security that are locked down to the general public for legal reasons. The three elements of concern are Social Security Number (SSN), race/ethnicity, and medical/disability. Because of the significance of the data, the data fields are available through most packages provided by Ellucian or created by the College of Charleston. This security section addresses the need to make the data available to the appropriate users and protect it from users not approved to access the data, while allowing minimal modifications and versions of packages to be made. Without this functionality, Information Services would need to maintain two copies of each package in which the data is made available by Ellucian.

Cognos accommodates our need to restrict this data to only allow access for people with permission to see/use it. The College will use a combination of Active Directory security groups, owned by the relevant data owners, and Framework Manager object security options to implement the appropriate security for the race/ethnicity and medical/disability fields. For more information on how Active Directory groups are used to secure the Cognos environment, go to the Active Directory section of this document. To secure the SSN, the DBAs and Information Services will work together to populate a table with users who have completed the appropriate legal documentation to allow for access to the full SSN.

Data Owners and AD Data Security Groups
Currently there are two elements of sensitive data that are secured using AD data security groups. The Center for Disability Services is the Data Owner for one of the two elements—medical and disability information related to students. The security group in Active Directory for these elements is called SG_MedicalDisabilityApprovedUsers. The Registrar and the Associate Director of Human Resources are the Data Owners for the other element—race/ethnicity for students or employees, respectively. The relevant security group in Active Directory is called SG_RaceEthnicityApprovedUsers. The College has an on-line form for users to request access to these data fields. The Data Owners approve access based on these form requests and maintain the lists in Active Directory.

Social Security Numbers
Social Security Numbers are secured by the College in a variety of ways, contingent upon the application. For a College employee to have access to the full SSN, a user must request access through a security form, his/her supervisor must sign-off on the form, and it is forwarded through a chain of approvers and ultimately is stored in Infrastructure. If a user has access to the full SSN for one area, he/she has access to the full SSN for all areas to which he/she has access already. Access to the full SSN is not data area specific. So, if a user in the Registrar’s Office has access to the student SSN for business purposes, and that user has access to Human Resources reports which include the employees’ SSNs, that user will be able to see the employee SSNs, as well.
Sharing Data or Reports
There are multiple reasons to use the Cognos Connection to share data or reports with other users. All of the security options outlined above add up to a very secure method for sharing, from the macro level of Finance or Student user, to the fine grained access of Fund, Organization, Account, and Program combinations.

The folder level security will ensure that only a person who has been approved for access to an area’s data will have access to reports contained within that area’s Report Folder. If a person has not been granted explicit permission to Student data, for example, she will not see the Student folder when she logs in to Cognos, even if she is a Finance user and can access other reports within the Finance folder. She must be granted access by the data owner and then entered in the student group of the CognosDataAccess_OU Student reports that are available, as well as having the Student Oracle Role assigned by the DBAs.

Because of the fine grained access level of security, sharing reports should be done using the Cognos interface. It will ensure that if two people can see the same report, only results specific to the user who is logged in will be returned.

The College of Charleston discourages sharing secure data via e-mail. The College provides shared drives, as well as FileLocker, which is a tool that allows for sharing a file with someone without needing to set up and maintain a secured shared folder. It gives the person who posts the file the ability to share it with the intended recipient and set security as needed for that particular file or group of files.

Through the use of Outlook and Cognos, along with other tools, College employees have the access to deliver any data to anyone; however, data security is a priority for the College. E-mail is not a secure method of sharing files. If a user e-mails the results of a report to someone, he is responsible for ensuring the data he is sending 1) is not sensitive data (SSN, grades, etc.) and 2) the person(s) to whom he is sending the report is an approved consumer of the data contained within the results and 3) is sent to the person intended. The College cannot prevent someone from emailing files to someone without access but it is the responsibility of the consumer to not do so.