

Two Portals, One Sign-On: Gateway to University Reporting

Ali Yorkos, University of Central Florida, Orlando, FL

Maureen H. Murray, University of Central Florida, Orlando, FL

ABSTRACT

Prior to the implementation of the university data warehouse and SAS® Business Intelligence (BI) software, our primary tools for information delivery were SAS Intr/Net® and a reporting database service. As the demand for more sophisticated information collection, analysis, and reporting has grown, the challenge has become how to deliver accessible data to administrators, decision-makers, strategic planners and the general university user community. This session chronicles the implementation and evolution of the SAS® Information Delivery Portal at a large university. The implementation included the development of a custom security integrator application to allow single sign-on access by users through the university's established portal and reconfiguring the SAS® Server software to use HTTPS. Also discussed is the security setup that controls what the users can access via their portal page. The SAS® Information Delivery Portal has become the common gateway for university users to access official data warehouse data, reports, processes and reporting tools.

WHO WE ARE

Mission

The mission of the Office of Institutional Research is to provide information of the highest quality and which is both timely and easily accessible and to facilitate and enhance decision-making, strategic planning, and assessment at the University of Central Florida. The scope of the unit's responsibility embodies the university, state and federal agencies, and the general public.

Purpose

Institutional Research (IR) provides electronic and web-based dissemination of official information to the University community (including the Board of Trustees, the various colleges, departments and other academic and administrative units), external agencies, and the Florida Board of Governors (BOG). IR generates, supervises or develops all official University data reports and state-required BOG reports, as well as providing end-user data solutions and training to facilitate the decision-making process. The director and staff serve on numerous university-wide committees and workgroups and assist with the collection and interpretation of institutional data, assist in planning academic programs, and participate in the implementation of evaluative procedures. The functions of the office support the entire university enterprise.

Background

Institutional Research has, as one of its primary objectives, the task of developing and implementing a university data warehouse. This enterprise-wide data system will facilitate the creation, access, and dissemination, by internal and external stakeholders, of institutional knowledge pertinent to the university. In collaboration with the data warehouse project stakeholder group, which represents a cross-section of key data users, the IR staff has established a data source of ten years' worth of student reporting data. This warehouse of information serves as the foundation for the development of a wide variety of reporting applications using SAS Business Intelligence software.

INTRODUCTION

The creation of our university data warehouse and the installation of SAS® Business Intelligence software expanded and upgraded our department's information collection, analysis and reporting capabilities. After a careful evaluation the department decided upon using the SAS® Information Delivery Portal as the university wide reporting and information dispersal mechanism. Due to university standards and constraints, the implementation of the SAS® Information Delivery Portal required modifications basic to the SAS Portal security design. We also developed and implemented the UCF security policy for the SAS® Business Intelligence software. The security policy implementation included modifications to the SAS BI delivered metadata. SAS consultants were engaged to implement the more sensitive modifications required for our enhanced SAS® Business Intelligence installation. This paper details our university's implementation and current use of the SAS® Information Delivery Portal as our gateway to university reporting.

VISION OF INFORMATION DELIVERY

Prior to the implementation of the university data warehouse and SAS® Business Intelligence (BI) software, our primary tools for information delivery were SAS Intr/Net® and a reporting database service. As the demand for more sophisticated information collection, analysis, and reporting grew, the decision was made to expand and enhance university reporting capabilities through the creation of a SAS® Data Warehouse and the use of SAS® BI software. Following the initial setup of the warehouse and conversion of some of the existing reports using SAS® Enterprise Guide®, the challenge then became how to deliver accessible data to administrators, decision-makers, strategic planners and the general user community. The SAS® Information Delivery Portal was determined to be the optimum solution to this problem.

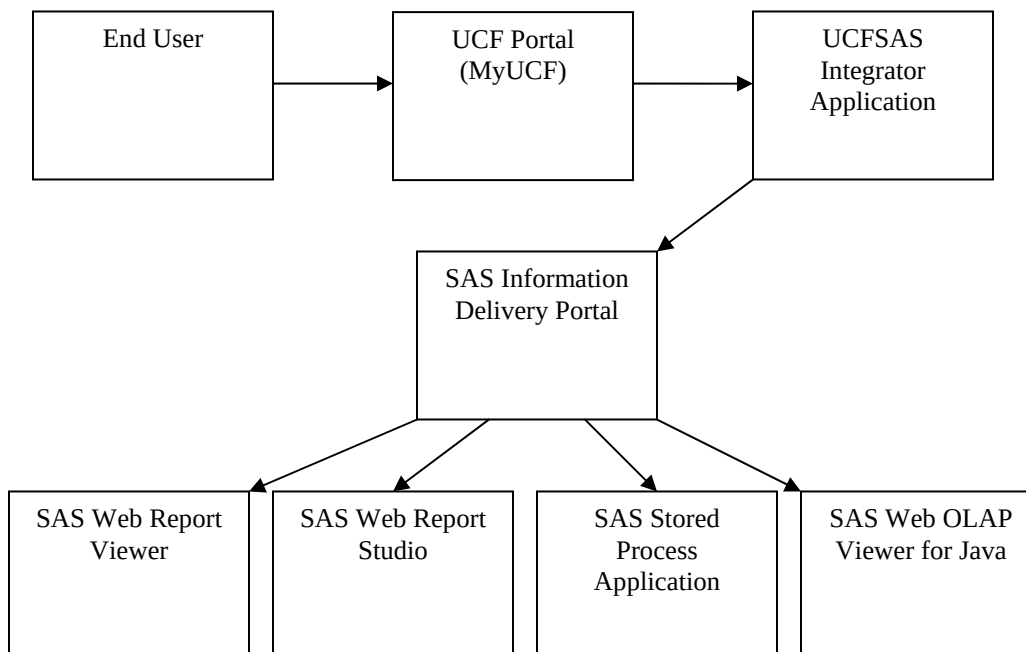
Why? We envisioned a platform to surface our varied types of information, ranging from newly developed stored processes to our classic yet sophisticated SAS Intr/Net® applications, still heavily relied upon by the university community at large, while the platform concurrently provided access to new and current reporting tools. This platform would need to evolve over time into our information gateway. The SAS® Information Delivery Portal (IDP) design focus is customization achieved through the use of different types of portlets and their contents. IDP portlets are used to organize report offerings, provide access to SAS and other reporting tools, and ease navigation to non Portal information sources through the use of links. Another advantage of IDP is the user's ability to customize their IDP pages, independent of any page provided by the IDP Administrator. Therefore, users can create personalized platforms which include whatever they need to acquire their required information such as the setup to run favorite or frequently required reports, links to non IDP websites and reporting tools.

IMPLEMENTATION OF INFORMATION DELIVERY PORTAL

Single Sign-On Functionality

For the past two years, the University of Central Florida has been in a portal environment for access to secure university data and information. During the initial planning for implementation of the SAS® Information Delivery Portal, it was decided that a single sign-on capability was needed so that the community of information users would not have to log in to two separate systems, each requiring a unique user ID and password. The proposed Application Architecture is as follows:

Figure 1: Proposed Application Architecture



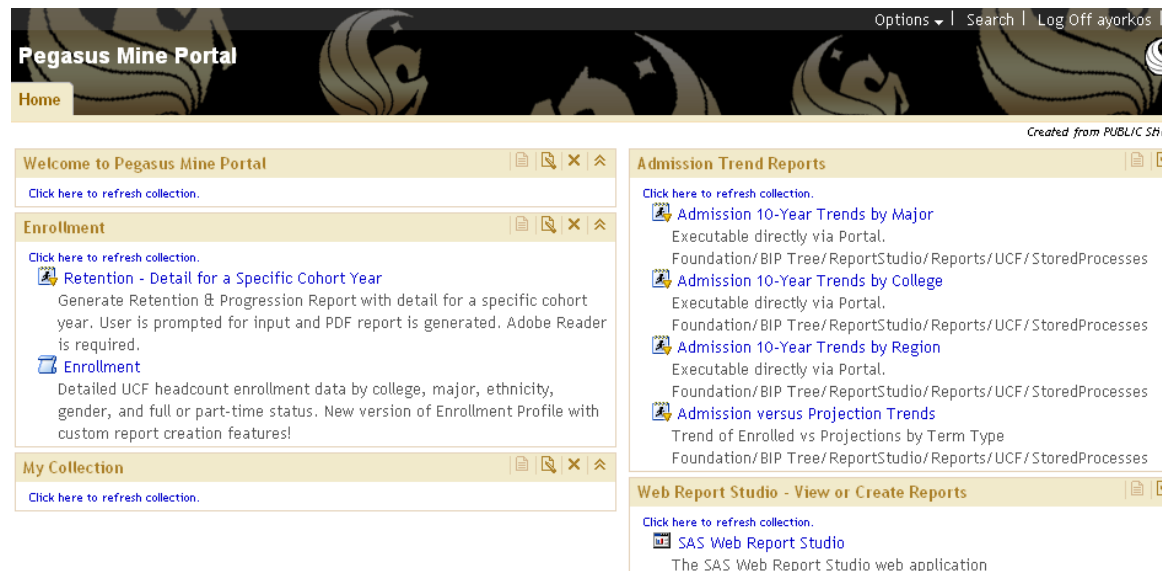
The end User requests access to the MyUCF PeopleSoft Portal environment. MyUCF performs the authentication and grants access if the user is valid. Once the user has been authenticated, the user is granted access to the MyUCF PeopleSoft Portal and the appropriate menu selections are made available. The user will have the ability to select the SAS® Portal link from within the MyUCF environment if the appropriate permissions have been enabled. The user will select the SAS® Portal link and will be directed to the UCF/SAS Integrator web application.

The web application validates the user request based on USER ID, TIMESTAMP, and HASH values passed from the MyUCF PeopleSoft Portal. A valid request is then forwarded on to the SAS® Information Delivery Portal. The SAS® Information Delivery Portal validates the USER ID against the current metadata environment and displays the appropriate content to the user. Based on metadata permissions, the user will have the ability to gain access to other SAS® Web Applications such as SAS® Web Report Viewer, SAS® Web Report Studio, SAS® Stored Process Application, and SAS® Web OLAP Viewer for Java.

Figure 2: MyUCF Portal page includes all available applications under “Staff Applications”. “Pegasus Mine Portal” link gives access to SAS® Information Delivery Portal.



Figure 3: Pegasus Mine Portal page includes all available SAS® Web Applications such as SAS® Web Report Studio and SAS® Stored Processes.



The IR project team collaborated with university computer services and web development staff to identify the possible solutions and determined that a custom integrator application would need to be developed. The application allows a user to log into the university portal and then by clicking on a SAS® Portal link which appears on the individual's home portlet page, the user's SAS® Portal home page opens in a new window! He or she can now access multiple SAS web applications and reports.

Custom UCF/SAS Integrator Web Application

The UCF/SAS Integrator Web Application was written in to act as a broker between the PeopleSoft user redirection module and the SAS® Web Applications. This bridge allows for the appropriate setup of session information prior to a user being passed into the SAS® Information Delivery Portal. The UCF/SAS Integrator Web Application validates the user request by processing the parameters, USERID, TIMESTAMP, and HASH, to ensure a valid request. Once the validity of the request has been established, the user is granted access to the SAS® Information Delivery Portal.

The following Web Application Archive was created to support the UCF Single Sign-On implementation:

- UCFSASIntegrator.war: This package contains the following elements:
 - index.jsp: This is a primary integration file for use by the PeopleSoft Portal as the redirector. It assumes that the SAS Information Delivery Portal® will not be launched within the PeopleSoft Portal wrapper.
 - IndexWrapper.jsp

Host Authentication to Trusted Web Authentication

Deploying the SAS Web Applications in a Trusted Web Authentication environment causes the following changes in the administration and access to SAS Web Applications:

Figure 4: Changes in the administration and access to SAS Web Applications

Required access	Host User Accounts on SAS Computer Server	Host User Accounts on SAS Metadata Server
SAS Web Application	No	No
SAS Web and Compute Application	Yes	Yes

The Trusted Web Authentication deployed at UCF is a customization made to the standard SAS software deployment and will exhibit the following differences, in addition to those listed above, from the standard Trusted Web Authentication:

Figure 5: SAS software deployment with Trusted Web Authentication

SAS Web Applications	Accessible via URL
SAS® Information Delivery Portal	No
Other SAS Web Applications	No

Secure Socket Layer Implementation

In order to secure our SAS® Information Delivery Portal as well as other SAS Web Applications, we performed the following steps:

1. Obtained an SSL certificate from a vendor that provides SSL certificates.
2. Installed the certificate onto the server.
3. Configured Tomcat server.xml file to work with the SSL certificate.
4. Configured SAS Web Applications to work with SSL.

Obtaining and Installing the SSL Certificate

The first step in obtaining a certificate is to generate a certificate request or a CSR file. In order to generate a CSR file, a functional keystore is created to make the key. This is done with the following command:

- **keytool -genkey -keyalg RSA -alias tomcat -keysize 1024 -keystore keystorename.kdb**

The requester will then be asked to fill in some fields. The first one is the common name, or domain name. Some versions of Java ask for first and last name, but the requester should put in a domain name. The only other fields required are the Organization name and the Country Code. At this point, a new keystore database has been created. The requester can now generate a certificate request, or CSR. It is very important that the requester use the exact same alias as he or she did when he or she made the key. This is done with the following command:

- **keytool -certreq -alias tomcat -file certreq.txt -keystore keystorename.kdb**

The requester then uses this CSR to process an order with a vendor. The requester should remember to include the "-----BEGIN" and "-----END" lines when doing so. When the order is complete, the requester will receive a new certificate that can be cut and paste into a text file. Before importing this certificate, the requester must import the Root Certificate for the order. The requester should then download the DER format to a working keytool directory, and proceed to type the following command (the file has to be renamed to something smaller and more manageable).

- **keytool -import -trustcacerts -file rootfilename.cer -keystore keystorename.kdb**

The requester should type in "yes" to import the file as a trusted authority. Finally, the server certificate is ready to be imported. If the requester is using a version of java below 1.4.2, he or she will need to convert this to binary or DER format. This can be done by copying it over to a windows machine with an extension of ".cer", double-clicking on it, going to the details tab, and "copying" it to a file as a binary DER formatted certificate. The command to import the server certificate is:

- **keytool -import -alias -tomcat -file certificatename.cer -keystore keystorename.kdb**

If the next message is "Reply inserted into keystore" after typing in the password, then the requester has successfully created a keystore database.

Configuring Tomcat Server.xml File

This file is usually located in **C:\Tomcat4.1\conf** folder on your server. Edit the file with Notepad or a similar editor. The configured file should look like this:

<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->

```
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
    port="8443" minProcessors="5" maxProcessors="75"
    enableLookups="true"
    acceptCount="10" debug="0" scheme="https" secure="true"
    useURIVValidationHack="false" disableUploadTimeout="true">
    <Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
        clientAuth="false" protocol="TLS"
        keystoreFile="C:/.../keystorename.kdb"
    />
</Connector> -->
```

The keystore file can be saved anywhere on the server as long as the script above in server.xml is correctly pointing to that file. After completing these configuration changes, the requester should be in business. For example, if the requester tries: <https://localhost:8443>, he or she should see the usual Tomcat splash page.

Configuring SAS Web Report Studio®

In order for WRS to work with SSL, a new Web Application link should be created for the portal Web Application. This is performed by running a **SASLoadWebApplication** utility that is located in **C:\Program Files\SAS\Web\Portal2.0.1\OMR** folder. The following changes should be made in the file using the organization specific security and meta-data parameters:

<pre>options metaserver="localhost" metaport=8561</pre>

```

metauser="saswbadm"
metapass="Admin123"
metarepository="Foundation";
%let groupOrUserName=PUBLIC;
%let identityType=IdentityGroup;
%let webappName=SAS Web Report Studio;
%let webappDescription=The SAS Web Report Studio web application;
%let webappURI=/SASWebReportStudio/logonFromPortal.do;

```

DATA WAREHOUSE USER ACCESS SECURITY POLICY

UCF's data warehouse access security policy, as an attempt to identify and organize our users, defined several functional personas(groups) each possessing different levels of security granted:

- **Administrators** - responsible for ensuring that the system is maintained and available while simultaneously secured appropriately. The Administrators have responsibility for the production server housing SAS applications and web software. Authorized SAS tools: SAS® Management Console.
- **Information Enablers** – responsible for creating and maintaining data warehouse target tables and provide any required user friendly data sources. Sensitive stored processes are controlled by this group to ensure they end up in the correct metadata location, which is properly secured to its intended audience. Authorized SAS tools: Data Integration Studio, Information Map Studio, OLAP Cube Studio, Management Console, and Enterprise Guide for stored process testing.
- **Stored Process Developers** – responsible for independent development of reports and analysis of information by utilizing Enterprise Guide with direct access to data tables. This group will have the ability to create SAS reports or stand-alone stored processes that stream or publish the output. Stored processes developed by this group cannot be published to the Information Portal. Authorized SAS tools: Enterprise Guide, SAS® Add-In for Microsoft Office and Web Report Studio.
- **Report Authors** - responsible for the analysis, reporting, and creating of information intelligence content. Authorized SAS tools: SAS® Add-In for Microsoft Office and Web Report Studio.
- **Information Consumers** - a read-only population of users generally interested in accessing the information content and reports created by the other personas quickly and consistently. Information Consumers will access information content exclusively via the SAS® Information Delivery Portal Authorized SAS tools: None.

The personas above are used to assign functionality to the varied university wide users. For example, the users within the College of Education will be assigned to the persona that best fits their need and function with respect to their college or department, resulting in EDUC Information Enablers, EDUC Stored Process Developers, EDUC Report Authors and/or Information Consumers.

METADATA FOLDER STRUCTURE MODIFICATIONS

In order to enforce process and data access security along business lines, the BI Metadata folder structure normally configured on the BIP Tree required modifications. Below is an example of the implemented structure using the College of Education.

```

ReportStudio
  Reports
    UCF
      Reports
      Maps
      StoredProcesses
    EDUC
      Reports
      Maps
      StoredProcesses

```

UCF related folders are used to hold reports, maps and stored processes that are available on a university wide basis. The EDUC related folders are used for the same type of objects but with access restricted to only EDUC users. Business line restrictions are implemented using the Access Control Templates (ACT). ACTs are configured and applied using the SAS® Management Console.

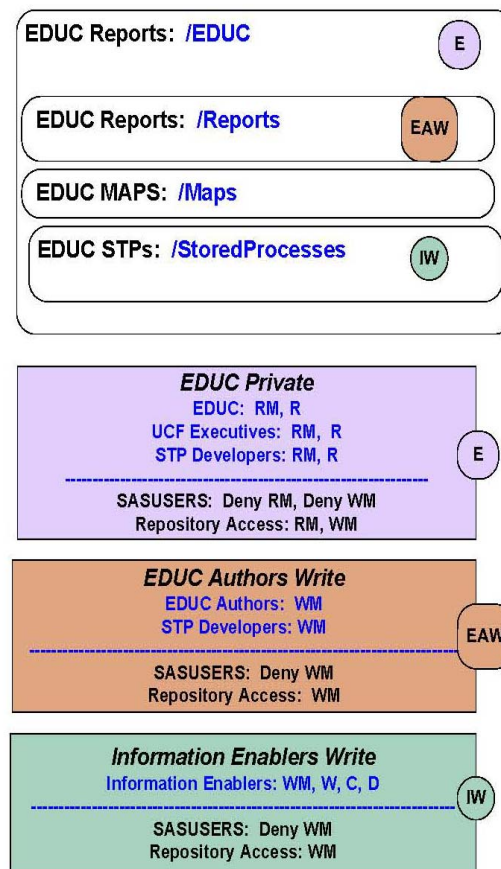
The Repository ACT grants global access rights. In figure 6 below the ACT's graphically displayed in the purple, tan and aqua boxes refines or limits the access granted by the Repository ACT. Therefore, when the EDUC Private ACT

(E) is applied to the /EDUC folder object only the user groups specifically listed in the EDUC Private ACT (EDUC, UCF Executives, and STP Developers) are granted Read and Read Metadata access to that folder. When the EDUC

Authors Write ACT (EAW) is applied to the EDUC /REPORTS folder object only the EDUC Report Authors group and Stored Process Developers are granted write metadata permission to the folder. Please note that EDUC Information Enablers is the only group with permissions to write metadata, write, create and delete to the EDUC

/StoredProcesses folder with the application of the Information Enablers Write ACT (IW). Figure 6 illustrates the application of Application Control Templates onto the EDUC folders segment of the BIP Tree.

Figure 6:



STORED PROCESSES SECURITY WITH RESPECT TO IDP

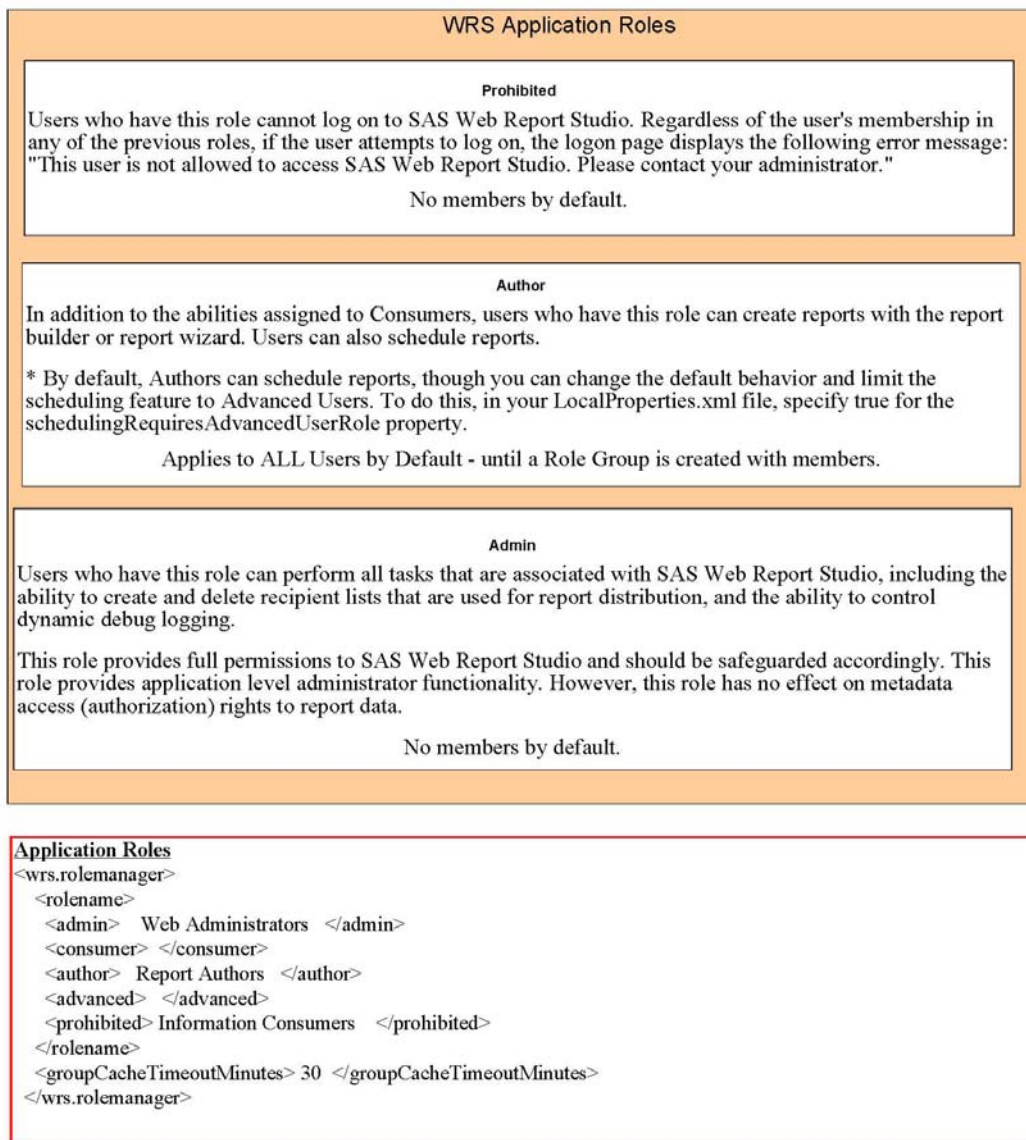
Stored processes are developed outside of the portal environment using Enterprise Guide. To ensure that stored processes are used in accordance with our security policy, all stored processes developed by the Stored Process Developer Personas are validated and registered by the Information Enablers or Administration personas to the Stored Process Server. Secondly, the placement of each stored process into specified folders ensure it can be found

and executed only by intended authors and consumers. If, for example, the stored process runs code against private EDUC data, only members of the EDUC user's group will have read permission to the folder where the stored process will be placed, and therefore only this group can see and therefore execute the stored process.

WRS SECURITY WITH RESPECT TO IDP

In respect to the IDP, all personas have access to SAS® Information Delivery Portal. However, Information Consumers are restricted to just the SAS® Information Delivery Portal without access to Web Report Studio. Figure 7 (below) depicts the Web Report Studio roles that have been implemented to date with the respective .xml tags used within the LocalProperties.xml file. Note how the Information Consumers group is prohibited from Web Report Studio even though a link to WRS is provided on the IDP home page. During the implementation of the single sign-on security measure the ability to access Web Report Studio via its' normal URL was blocked, this ensures the only access to WRS is via IDP.

Figure 7:



EXAMPLES OF REPORTS AND FUNCTIONS SURFACED ON OUR IDP

The SAS® Information Delivery Portal has evolved into the common gateway for all our user groups to access official data warehouse data, reports, processes and reporting tools. The tools and functionality now easily accessible by the user community include stored processes, Web Report Studio/Viewer, and OLAP Cubes viewed via the Data Explorer Viewer.

An example of an application successfully converted during this implementation process is the university Enrollment Profile which previously had been a drillable web-based process providing varied views of enrollment data, including student classifications, gender, residency, ethnicity, and full time/part time status by college or major. This extensive process was converted utilizing the SAS OLAP Cube Studio® and is accessed using the Data View Explorer via an Information Map icon on the IDP. Also, the web-based Student Retention Analysis process which creates retention and progression data reports and delivers this data via Adobe PDF or Excel files has been converted to a stored process surfaced via the IDP.

Examples of newly developed stored processes are Admissions Geographic Profile and Admissions Trend Analysis, both developed with Enterprise Guide. The Admissions Geographic Profile stored process presents 10 years of admission profile data with drill down capability, allowing a parameter selection of either summer, fall or spring terms. The Admissions Trend Analysis stored process graphically displays the projected versus actual student admits across multiple academic terms, with providing a parameter selection of terms. A variety of Enterprise Guide's graph options such as line plots, pie charts, and 3-D vertical bars graphs are used to visually enhance formatted reports.

CONCLUSION

The IR development team in collaboration with the data warehouse stakeholders group continues the development and enhancement of delivery options and functionality within the SAS® Portal. For example, the functionality of each of the older SAS Intr/Net® applications is under evaluation to determine which BI tool is most appropriate for its conversion to allow availability through the IDP. The implementation of the SAS® Information Delivery Portal and the achievement of single sign-on access enabled the IR Office to meet the challenge of providing easily accessible data and dynamic reporting to the university community.

REFERENCES

SAS® 9.1.3 Intelligence Platform Administration Guide.

SAS® Web Infrastructure Kit: Administrator's Guide.

ACKNOWLEDGMENTS

We sincerely acknowledge several SAS consultants who provided help and support during our implementation of the SAS® BI Platform. This paper references documentation developed by these SAS consultants.

CONTACT INFORMATION

Your comments and questions are valued and encouraged. Contact the authors at:

Maureen Murray
Office of Institutional Research
University of Central Florida
P.O. Box 160021
Orlando, FL 32816-0021
Work Phone: (407) 823-4764
Fax: (407) 823-4769
Email: mamurray@mail.ucf.edu
Web: <http://www.iroffice.ucf.edu>

Ali Yorkos
Office of Institutional Research
University of Central Florida
P.O. Box 160021
Orlando, FL 32816-0021
Work Phone: (407) 823-4764
Fax: (407) 882-2314
Email: ayorkos@mail.ucf.edu
Web: <http://www.iroffice.ucf.edu>

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration.

Other brand and product names are trademarks of their respective companies.