|  |
| --- |
| my.harvard Distributed Security Model |
| Access Procedures |
|  |

Updated 8/16/2017

Contents

[Introduction 2](#_Toc490663596)

[PeopleSoft Campus Solutions Security Overview 2](#_Toc490663597)

[Password Controls 3](#_Toc490663598)

[Logging On 3](#_Toc490663599)

[Passwords 3](#_Toc490663600)

[Batch IDs 3](#_Toc490663601)

[Access Procedures 4](#_Toc490663602)

[User Creation 4](#_Toc490663603)

[Manual Role Assignment Process 4](#_Toc490663604)

[How to Add/Remove a Role on a User’s Profile 6](#_Toc490663605)

[Dynamic Role Assignment Explained 11](#_Toc490663606)

[Data Security 11](#_Toc490663607)

[How to Add/Delete Data Security 18](#_Toc490663608)

[Transfer User Process 26](#_Toc490663609)

[Access Roles 26](#_Toc490663610)

[Role Modifications / New Roles 26](#_Toc490663611)

[Non Production Environments 26](#_Toc490663612)

# Introduction

The purpose of this guide is to outline the my.harvard security model. The my.harvard site is now live primarily supporting the following schools and areas:

* Faculty of Arts and Sciences (FAS)
  + Harvard College (HCOL)
  + Graduate School of Arts and Sciences (GSAS)
* Harvard Divinity School (HDS)
* Harvard T.H. Chan School of Public Health (Harvard Chan)
* Harvard Graduate School of Education (GSE)
* Harvard Graduate School of Design (GSD)
* Harvard Kennedy School (HKS)
* Student Financials (university-wide) (SFS)

The my.harvard system includes the Campus Solutions (admin) and Interactive Hub (portal) applications. The Campus Solutions application is accessed via the https://admin.my.harvard.edu web address. These users accessing this link are categorized as “Back Office Users”. This will include users from the Student Financials Office, each school’s Registrar’s Office as well as other groups defined by each school. The Interactive Hub is accessed via the https://portal.my.harvard.edu link. These users are categorized as “Portal Users” and will include advisors, faculty and students. The portal side has a polished look and feel featuring simplified navigations. The portal and admin sites are connected.

In each section, you will first read about the production environments’ policy. Where applicable, there will also be a following comment regarding the nonproduction environments. To find the current links to these environments please navigate to <https://nonprod.my.harvard.edu>. This link will only work if you’re currently logged on to VPN. The nonproduction environments include P-2 (Test), P-1 (INT), and Prod 2.

# PeopleSoft Campus Solutions Security Overview

At a high level, PeopleSoft Campus Solutions security is made up of four elements: Permission Lists, Roles, User Profiles and Data Security. Permission Lists define permitted actions on security objects such as pages, queries and web services to name a few. These permission lists are grouped into roles that are assigned on the User Profile. Separately, users are assigned data security.

**Roles** serve as a functional grouping of security permission lists. A simple way to think of roles are a mechanism that determines where a user can navigate in the system, what sort of actions they can perform (View Only, Update, Add, Correct History). **Data security** defines what data is accessible on the navigations a user can access. While these are assigned separately, roles and data security work in tandem to provide the user with the necessary privileges. Included below, is a glossary of the terms mentioned in this section.

|  |  |
| --- | --- |
| **Key Terms** | |
| **User Profile** | A component within PeopleSoft that identifies the user ID, roles and user level permission lists. User profiles are automatically set up for employees at Harvard through a nightly process. Contractors must be set up manually for the interim while the SIS Team works on a more automated solution. |
| **Role** | A grouping of permission lists that provide access to a particular function. Roles will be designed by the Central Security Administrator at the request of SIS Team, Subject Area Approvers, and School Implementation teams. |
| **Permission List** | A list that defines security to pages, query records, processes, etc. On the my.harvard system permission lists will have a one to one relationship per page or object grouping. |
| **Data Security** | Referred to as Row Security in PeopleSoft, this when exercised restricts the data returned when a user inputs search criteria into a component. In some cases it can also restrict actions taken on a page. Data security is broken into numerous categories including Academic Career, Academic Org, Academic Programs, etc. |

# Password Controls

## Logging On

Users sign on to my.harvard through HarvardKey. There are a few exceptions. Batch IDs will be able to bypass HarvardKey by signing on through the PeopleSoft native logon screen. In order to access the alternate sign-on page, CyberArk, users must be logged to the SIS Admin or SIS Team VPN tunnel.

In some of the lower environments the logon procedures will be different. All users will utilize the PeopleSoft native logon screen in the P-2 (Test) and Prod2 environments. The P-1 (INT) site uses HarvardKey.

## Passwords

Since most users will sign on with their Harvard Key they will not need a password stored on their user profile. However, for the users (BATCHIDs) logging via the alternate sign-on page, CyberArk, a password will be required.

Any time a user is set up to logon via the PeopleSoft native logon screen, mostly in the lower environments, the initial password or password reset will be sent securely via Accellion. This process is followed for all environments.

## Batch IDs

Batch IDs will be utilized by groups on the my.harvard application to schedule and run processes. The current model is one batch ID per functional area on the SIS project and one per school. Currently this is the listing of Batch IDs:

|  |  |
| --- | --- |
| **Batch ID** | **Description** |
| FASBATCH | FAS Registrar Office |
| GREENBATCH | Student Financial Services Office |
| GSDBATCH | GSD Registrar Office |
| GSEBATCH | Harvard GSE Batch Registrar Office |
| HDSBATCH | HDS Registrar Office |
| HKSBATCH | HKS Registrar Office |
| CHANADBATCH | Harvard Chan Admissions Office |
| HSPHBATCH | Harvard Chan Registrar Office |

As mentioned earlier, users that logon to the my.harvard system that do not use HarvardKey will have to be on a two-factor VPN tunnel known as SISAdmin or SISTeam. Once signed-on, the user will open the CyberArk web application to negotiate the connection to my.harvard. Users must use their central account ID (3 letter 3 digits) and their Harvard Key password credential to access Cyber Ark. This tool allows the central security admin to easily reset the password for these batch IDs without disrupting the Batch ID’s users. Also, this method tracks who logged on with the batch ID.

Access role modifications may happen from time to time as new processes are developed or transitioned to the schools to run. To request or modify access for a batch ID, send an email [sis\_security@harvard.edu](mailto:sis_security@harvard.edu) with information on which batch ID(s), the page(s), and why this access is needed.

# Access Procedures

## User Creation

User Profiles are created each night at 10:30 PM. The process reviews the data loaded to my.harvard by HR and creates user profiles for new Harvard employees. Newly admitted students are also picked up at this time and profiles are built. Temporary staff will not be picked up by this process. These users will be built manually. To request access for a POI/Contractor, send an email [sis\_security@harvard.edu](mailto:sis_security@harvard.edu) with the following information: full name, HUID, email, and roles that should be added. Users will not be able to access the system without roles assigned on their user profile.

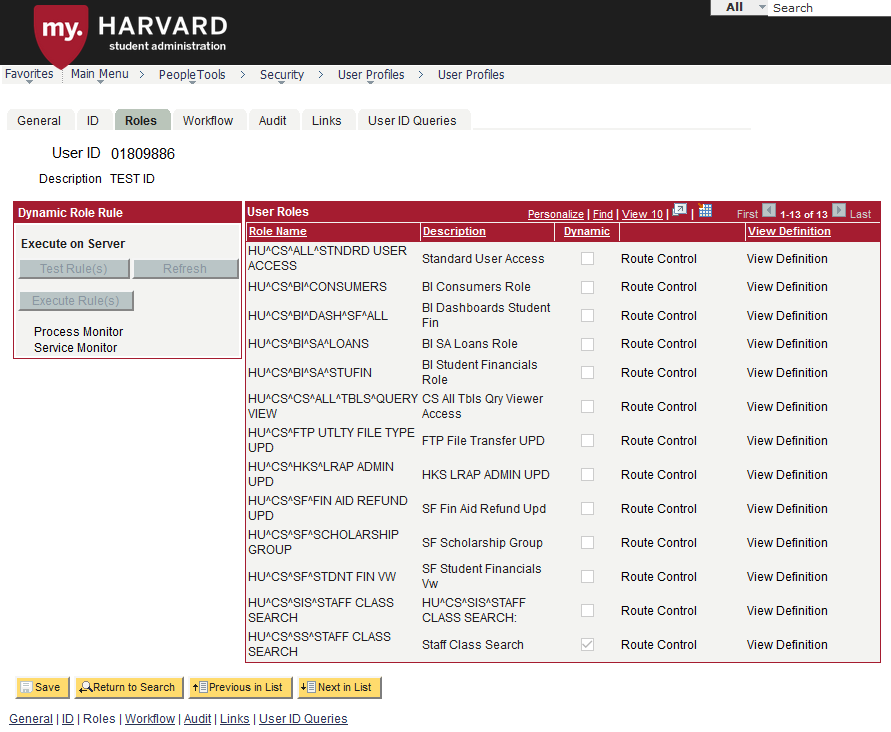
## Manual Role Assignment Process

Once a user profile has been set up, Local Security Administrators at each school can assign roles manually to a user. A best practice is to track all manually assigned roles through ServiceNow; some roles may be subject to an audit review by PWC.

Central Security Administrators become involved only when restricted roles or questions arise. If an access request originates to the sis security group first, the Central Security Administrator will pass on the request to the Local Security Administrator.

**Note: A full list of a user’s roles (including restricted roles) can be viewed on the user profiles page.**

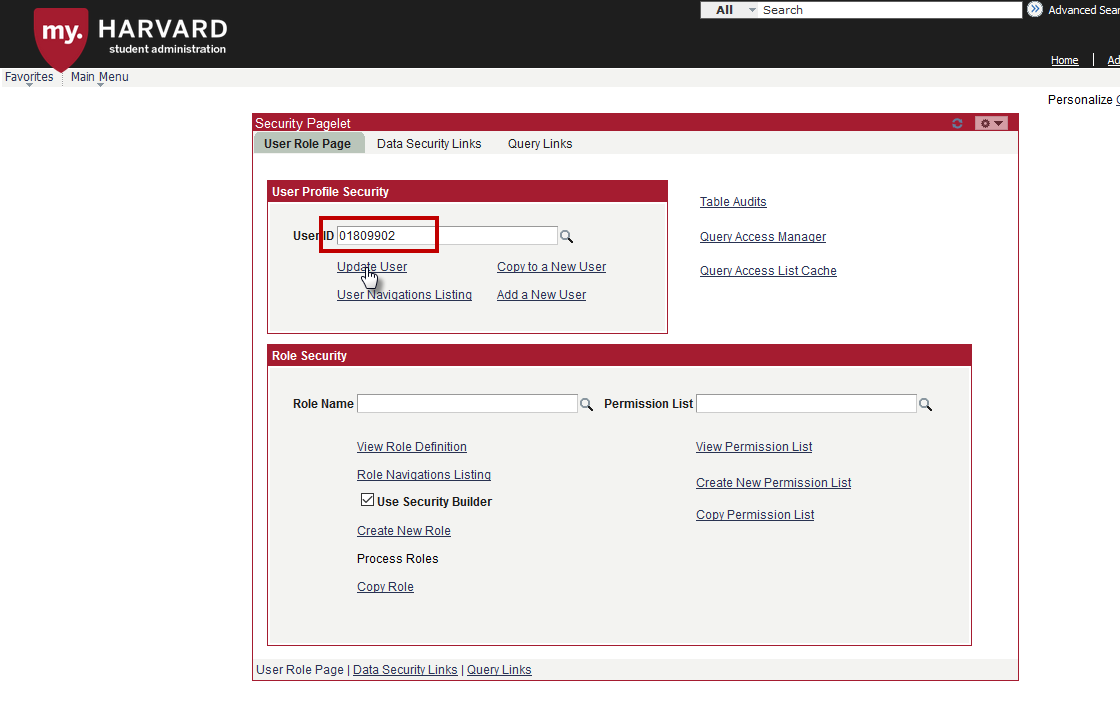
* Navigate to **PeopleTools > Security > User Profiles > User profiles.**
* **Enter the User’s HUID or full name if searched by description.**
* **Click on the Roles tab to view the full list of roles.**



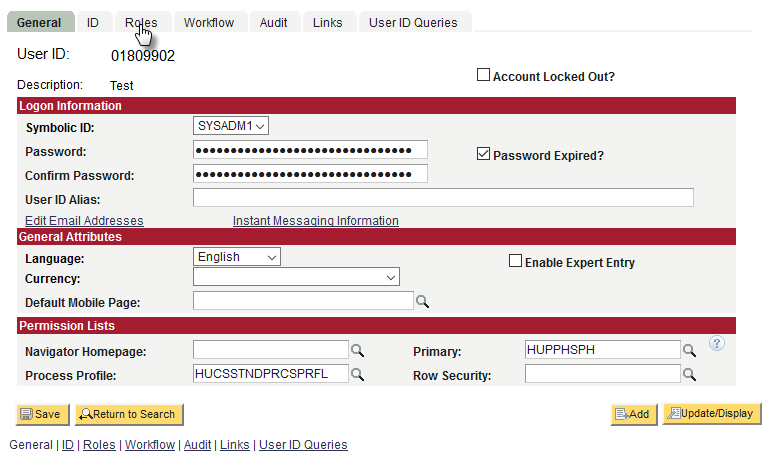
Manually assigned roles will be exempt from the dynamic role process; this process will be expanded upon in the next section. However, these roles can be removed manually or by the Terminated User Process. See an up to date list of all Security Administrators here: <https://cs.fss.finance.harvard.edu/my.harvard>.

## How to Add/Remove a Role on a User’s Profile

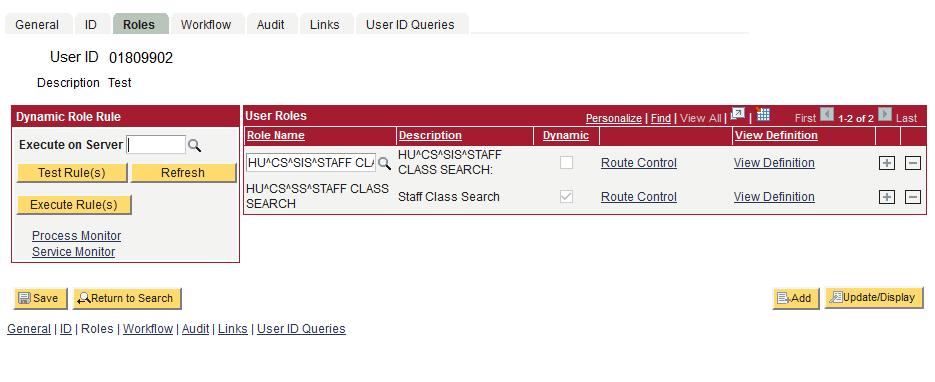
Navigate to the Security Pagelet on the home page. Under the **User Role Page** tab, enter the user’s HUID in the search bar. Click **Update User**.



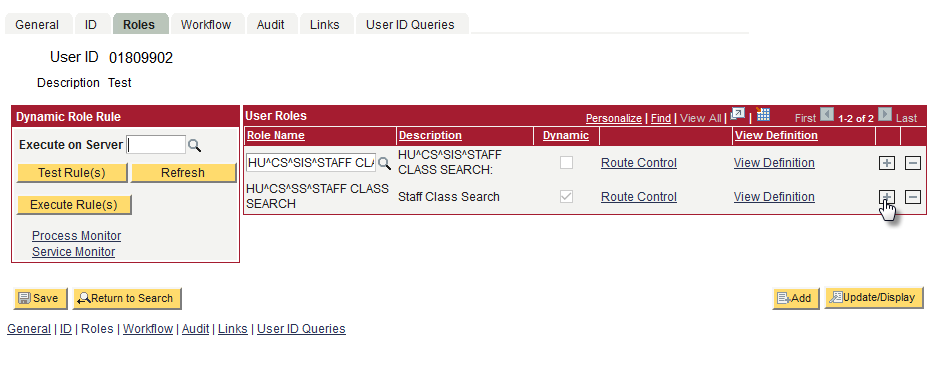
The user’s user profile will appear. Click on the **Roles** tab to modify the user’s roles.



The user’s current roles will appear. School security administrators will not be able to see roles they do not have access to grant.

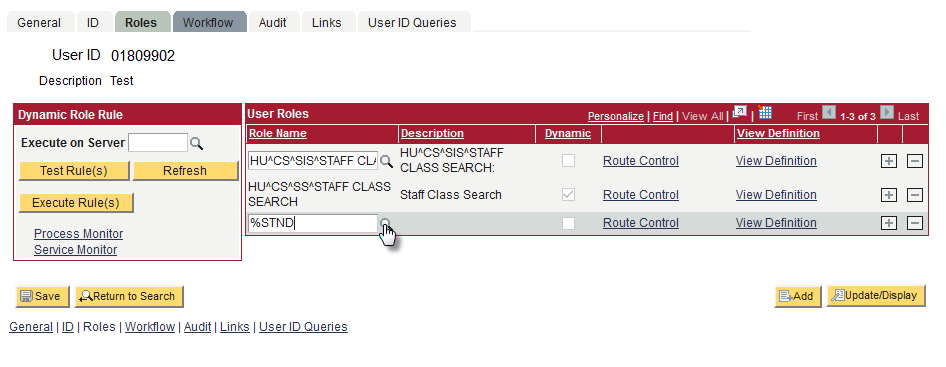


Click on the  to add a new row.

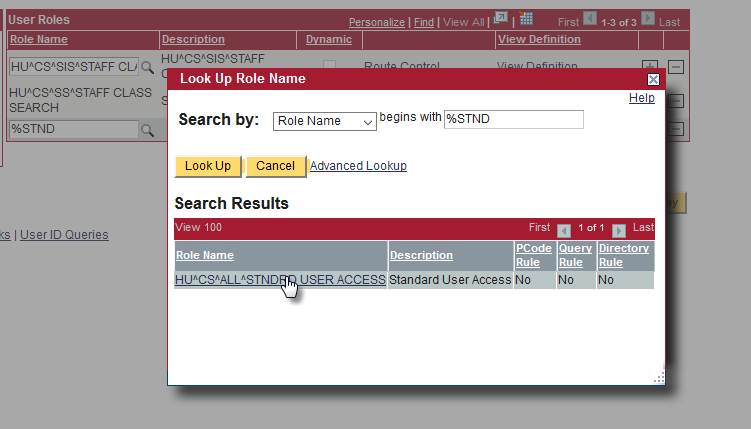


Enter the role name.

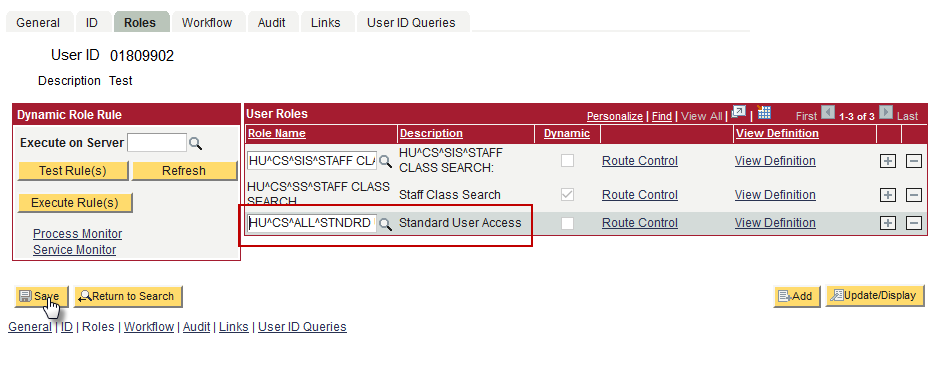
A role name can also be partially entered by putting the wildcard **%** in front of it. Click on the magnifying glass to search for the role.



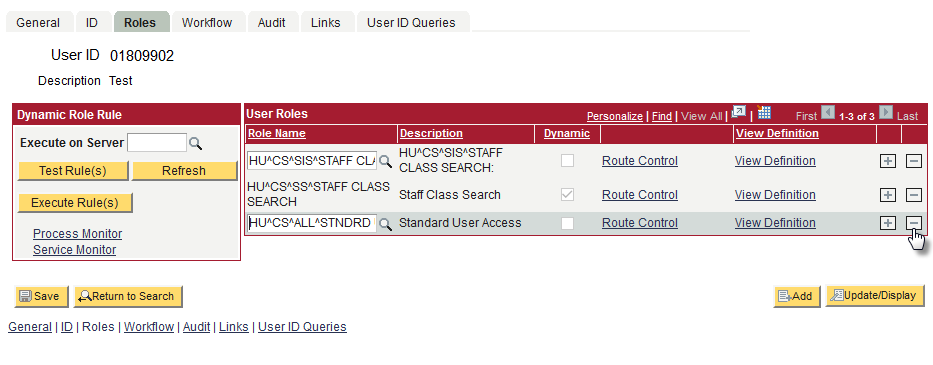
A list of roles will appear. Choose the correct role.



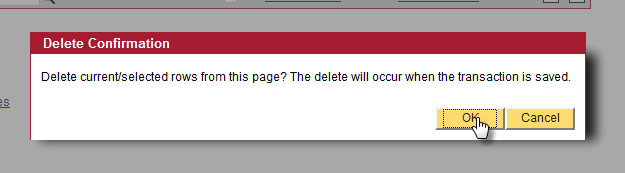
The role is now added to the profile. Click **Save** to save the changes.



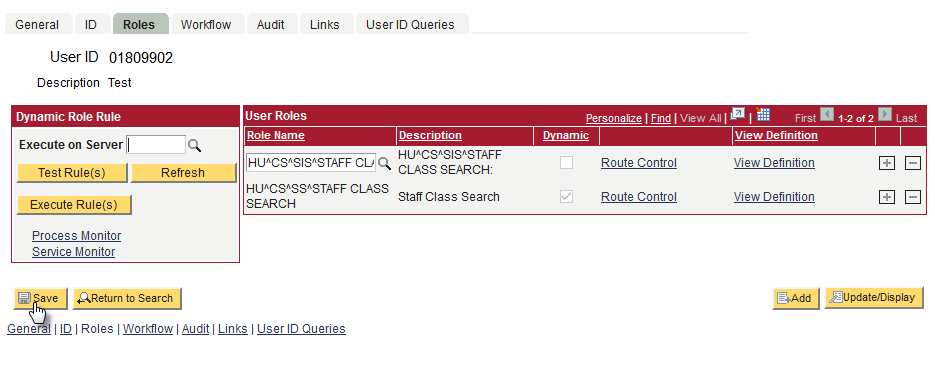
To remove a role, click the  on the role you wish to remove.



A confirmation message will appear. Click **OK** if you wish to proceed deleting the role.



The role has now been deleted. Click **Save** to save the changes.

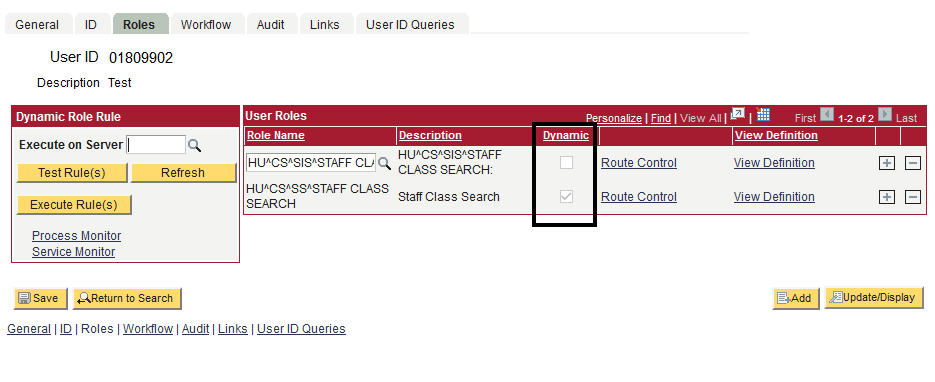


## Dynamic Role Assignment Explained

PeopleSoft provides a simple method to dynamically assign roles. A query is created to identify a population of users that meet specific criteria. For example, a query may identify all the active degree students at Harvard College. Every time the dynamic role process is run, the Harvard College Degree Student role is assigned to those users meeting the criteria. The process can be scheduled or run on an ad hoc basis. In addition to adding roles, the process will also remove the roles previously assigned dynamically when the user no longer meets the conditions.

All of the roles used for the portal users are assigned dynamically. This includes the Student, Faculty and Advisor permissions. Currently, the Dynamic Role process is scheduled to run every 6 hours starting at midnight. However, this may be scheduled to run more frequently during peak times of the year. The process can be run ad hoc when necessary.

School Security Administrators can tell if a role has been dynamically assigned to a user by checking the user profile. If the role is greyed out and has the box in the Dynamic column checked, the role is a dynamic role.



## Data Security

Data security will primarily be administered by the Local Security Administrators. It should be considered in conjunction with access requests. **Especially with new users, Academic Career and Academic Org should always be considered when processing an access request.**

Most of the configuration options for data security exist to either limit the user to accessing particular student populations such as students in a particular school (Institution/Campus Security), or in a particular program (Academic Program security), limit the data about a student that is presented such as test scores (Test ID security), or control data that can be associated to a user (Service Indicator Security).

Administration of data security involves a lot of maintenance, but fortunately security can be cloned from one or more users as will be illustrated later in this document. A table of all data security categories and their definitions can be found at the end of this section.

**Institution Security**

The highest form of data security utilized to control what student population a user can access is Institution Security. Institution is a typical required search field for pages presenting student data. All new users are automatically granted HRVRD Institution when their profile is created. If a user has been previously terminated, this field must be re-added when granting new access.

**Campus Security**

Campus security generally equates to the college or colleges whose data a user can access. This is also one of the more common fields to secure search pages and queries by, although probably not as common as Career (School). Campus security is only needed when giving access to curriculum.

The College (Campus) values as of this writing are:

|  |  |
| --- | --- |
| **Campus** | **Description** |
| ART | American Repertory Theater |
| BURSR | Bursar's Office |
| DCE | Div of Continuing Education |
| FAS | Faculty of Arts & Sciences |
| GSD | Graduate School of Design |
| HBS | Business School |
| HDS | Divinity School |
| HGSE | Graduate School of Education |
| HKS | Kennedy School of Government |
| HLS | Law School |
| HLSG | Law School - Graduate |
| HMS | Medical School |
| HSDM | School of Dental Medicine |
| HSPH | School of Public Health |
| NONH | Non-Harvard |

**Career Security**

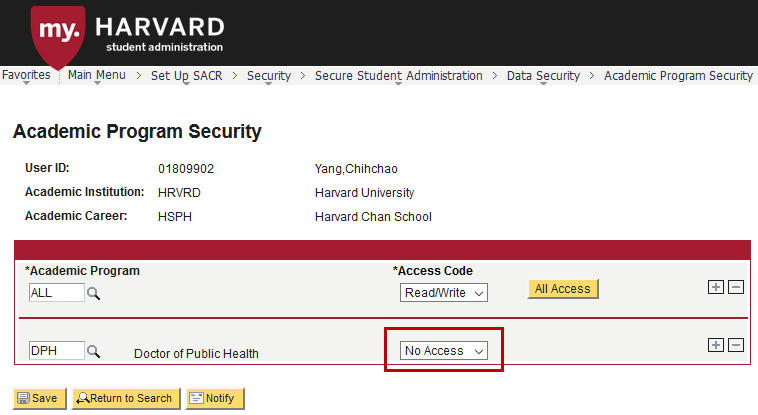
Career security generally equates to the school or schools whose data a user can access. This is the most typical form of data security used to secure search pages and queries by. Career level security drives OBI and ODS, and is needed for users needing access to CPP stacks.

The School (Career) values as of this writing are:

|  |  |
| --- | --- |
| **Academic Career** | **Description** |
| ART | American Repertory Theater |
| DCE | Div of Continuing Education |
| FAS | Faculty of Arts and Sciences |
| GSAS | Graduate Arts & Sciences |
| GSD | Graduate School of Design |
| HBSD | Business School Doctoral |
| HBSM | Business School MBA |
| HCOL | Harvard College |
| HDS | Divinity School |
| HGSE | Graduate School of Education |
| HKS | Kennedy School of Government |
| HLS | Law School |
| HLSG | Law School - Graduate |
| HMS | Medical School |
| HSDM | School of Dental Medicine |
| HSPH | School of Public Health |
| NONH | Non-Harvard |

**Program Security**

Academic Program security equates to the degrees by which a user is allowed to view students. Academic Program is also used to secure search pages and queries by, and required for users needing access to CPP stacks. Access to academic programs is dependent on Career security and both fields in conjunction can be used to secure student data. A user may be limited to the programs in only one Career or can view programs across multiple or all Careers. To view any program though, the user has to have access to the Career it is associated with. If a user should have access to all, or most of, the programs in a Career, an all option is provided to provide easy access. If specific programs should not be accessible, they can be included as individual rows with the **No Access** option selected.



**Plan Security**

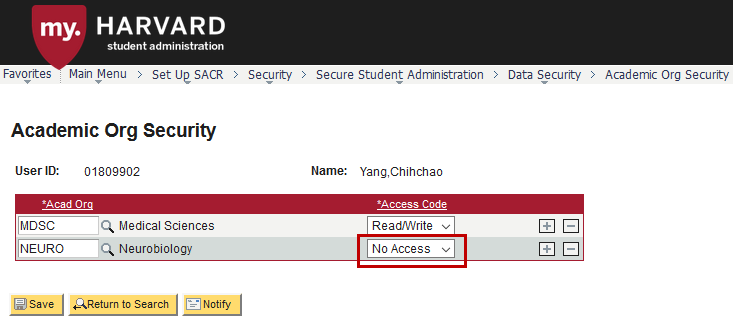
Academic Plans generally correspond to Majors. Plans are associated to the Institution in security not to Academic Programs. However, the ACAD\_PLAN\_TBL does associate plans to Academic Programs, Plan Types, and Degrees, any of which could be used as a grouping field to define plans a user would need access to.

Academic Plan security can also be applied to search pages and queries just like the previous fields, and is also needed for users needing access to CPP stacks. All access can be defined for plans across the Institution and specific plans flagged as No Access just like with Academic Programs.

**Academic Org Security**

Academic Org security is also often referred to as Class Permissions. It is security administered from a tree structure that organizes a University’s Academic Organizations into a hierarchy to easily grant and deny access to large numbers of orgs in a logical, easy to maintain manner. This security is used to support the schedule of classes and to secure course and course catalog setup pages.

**By granting access to a specific node of the ACAD\_ORGANIZATION tree, the security administrator is also implicitly granting access to all nodes in lower levels below it in the hierarchy. Individual nodes within a granted node can be set to exclude access (No Access) to refine the security to specific needs. Academic org security is key for any curriculum access.**



**Admissions Action Security**

This security screen controls the Admissions Program Actions a user can view or choose from. Admissions Action is independent of Institution, Campus, or Career.

The following are the current Admission Actions:

|  |  |
| --- | --- |
| **Admissions Action** | **Description** |
| Admit | Admit |
| Adm Revoke | Admission Revocation |
| Applicatn | Application |
| Cond Admit | Conditional Admit |
| Data Chg | Data Change |
| Defer Decn | Defer Decision |
| Defer Enrl | Defer Enrollment |
| Intent Mat | Intention to Matriculate |
| Deny | Deny |
| Matriculat | Matriculation |
| Plan Chg | Plan Change |
| Prog Chg | Program Change |
| Readmit Ap | Readmit Application |
| Reconsider | Reconsideration |
| Adm W/drwl | Administrative Withdrawal |
| Waitlist | Waitlist |
| Wait Offer | Waitlist Offer |
| App W/drwl | Applicant Withdrawal |

**Program Action Security**

This security screen controls the Program Actions a user can view or choose from. Program Action is also independent of Institution, Campus, or Career.

**The following are the current Program Actions:**

|  |  |
| --- | --- |
| **Program Action** | **Description** |
| **Activate** | **Activate** |
| Adm Revoke | Admission Revocation |
| Completion | Completion of Program |
| Data Chg | Data Change |
| Defer Enrl | Defer Enrollment |
| Discontinu | Discontinuation |
| **Dismissal** | **Dismissal** |
| Matriculat | Matriculation |
| Plan Chg | Plan Change |
| Prog Chg | Program Change |
| **Readmit** | **Readmit** |
| Revoke | Revoke Degree |
| Suspension | Suspension |
| Discontind | Voluntarily Discontinued |
| Adm W/drwl | Administrative Withdrawal |

**Application Center and Recruiting Center Security**

Access to view and update prospect and applicant data is controlled by Recruiting Center and Application Center security. Core Admissions pages will use this security to control rows returned on the search pages. Some of the primary admissions tables are delivered with Application Center security associated to them in the Query tools. As of this writing, no Recruiting Centers are defined. **While the associated Career is shown for the Application Center if it is defined with one, security cannot be performed by choosing Career and gaining the Application Centers associated to it. It shows as informational only. Application center security also feeds in to OBI for admissions subject areas.**

**Test ID Security**

Test ID security controls the test scores a user can see in the Test Results and Academic Test Summary pages. It also controls access into the External Test Score Load and Suspense pages, Search/Match/Post Test Scores pages, External Test Score Purge, and Test Score Candidate Date pages, by limiting the Test IDs the user can select from on the search pages. Test ID **security also feeds in to OBI for admissions subject areas.**

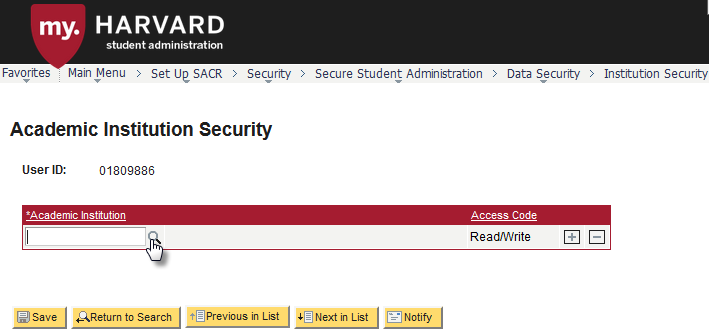
| **Data Security Category** | **Definition** |
| --- | --- |
| **Institution Security** | Authorizes access to Institutional data |
| **Campus Security** | Authorizes access to Campus |
| **Career Security** | Authorizes access to Careers |
| **Program Security** | Authorizes “all” or specific programs to a user. User cannot change a student’s program without security to that program. |
| **Plan Security** | Authorizes Plan security to users |
| **Academic Org Security** | Authorizes access to specific departments and Schools |
| **Admissions Action Security** | Authorizes Admission Actions used to process a student’s application and progress through the application process |
| **Program Action Security** | Authorizes Program Actions used on Student’s Program/Plan page - identifies the status: Active, Discontinued, or Completed. |
| **Application Center Security** | Authorizes access to Application Center by Institution |
| **Recruiting Center Security** | Authorizes access to Recruiting Center by Institution |
| **3C Group Security** | 3Cs (Comments, Communications and Checklists) are a flexible way to track and analyze correspondence, lists of requirements, and notes about the students, staff, and external organizations in the PeopleSoft database.  **Comment Management–** enables you to enter notes in the database about individuals, organizations, or events.  **Communication Management–** enables you to manage the institution’s incoming and outgoing contacts with students, prospects, recruits, staff, alumni, donors, and organizations.  **Checklist Management–** enables you to create lists to track activities and dues dates, and identify their status at any time. |
| **Service Indicator Security** | Provide or limit access to services for a student. Service Indicators can be holds that prevent a student from receiving certain services or positive indicators that designate special services to be provided. |
| **Advisement Report Security** | Authorizes access to advisement reports. Defines the user’s access to advisement reports based on each of their academic institutions. |
| **Student Groups Security** | Student Groups enables you to define groups of similar students at a high-level. Creating groups of students enables you to track and use the students within a group for campus-wide processing, such as billing, academic advising, etc. |
| **Transcript Type Security** | Authorizes access to transcript types (Unofficial, Official, etc.) |
| **Transcript Report Security** | Authorizes access to transcript reports |
| **Graduation Status Security** | Authorizes access to Graduation Review Status |
| **Milestones Security** | Authorizes access to milestones on a student. Access can be defined as update or inquire only. |
| **Test ID Security** | Authorizes access to Test Ids (Examples include GRE, SAT, TOEFL) |

## How to Add/Delete Data Security

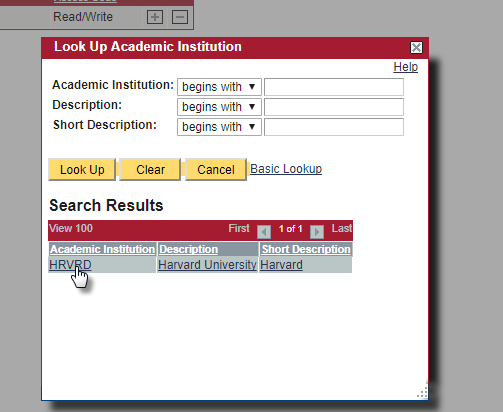
Navigate to the Security Pagelet on the home page. Under the **Data Security Links** tab, enter the user’s HUID in the search bar. Click on desired data security link.



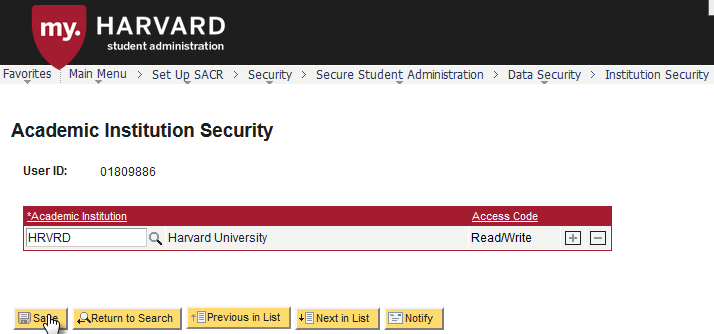
The user’s current data security will appear. Enter the desired data security. Clicking the magnifying glass will show all available options.



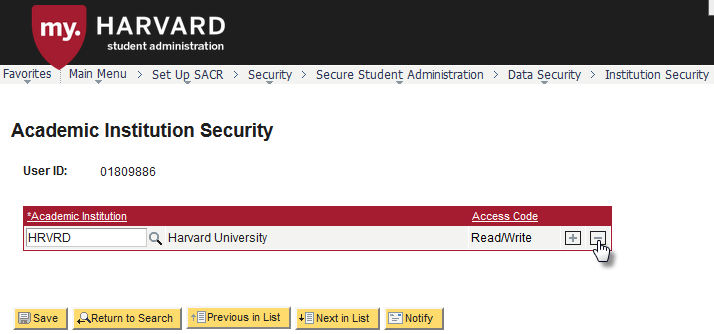
Select desired data security. For this example, HRVRD is the only option for academic institution.



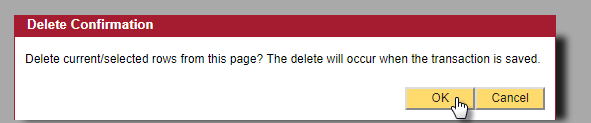
The chosen data security will populate. Click **Save** to save the changes.



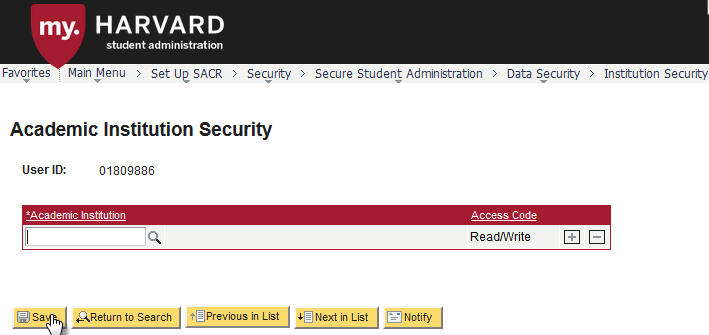
Data security can be deleted by clicking on the  sign.



A delete confirmation will appear. Click **OK** if you wish to continue with deleting the data security.



The data security will no longer appear on the user’s table. Click **Save** to save the changes.

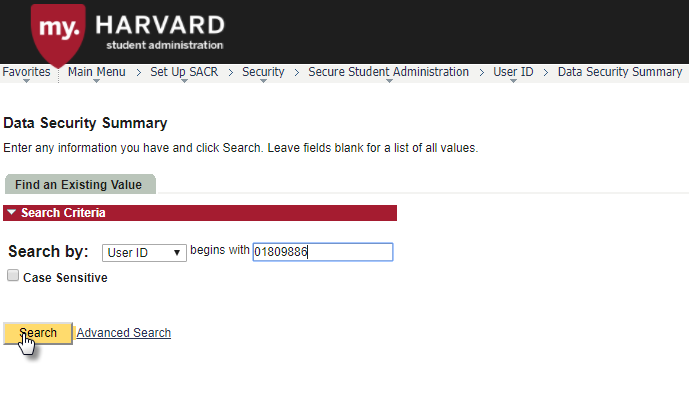


**Data Security Replacement**

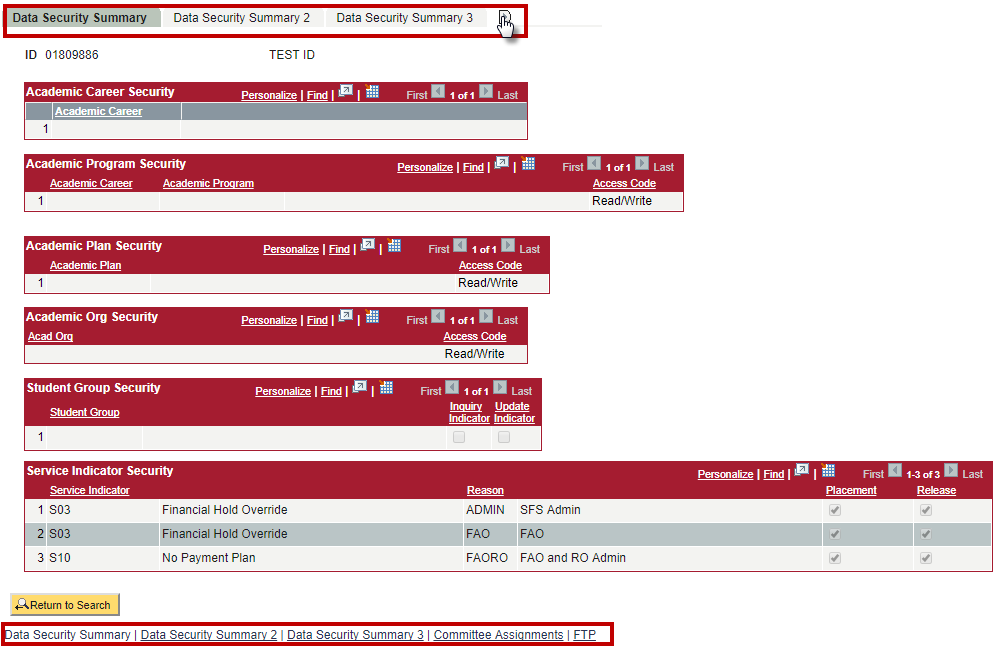
There is also a way to mass assign data security to a user by copying another user’s data security.

**PLEASE NOTE: This method will delete any current data security and replace it with the person’s data security that is being copied.** **Be sure to perform an analysis of the user’s data security to determine if any existing access should remain that the other user does not currently have.**

Navigate to **Set Up SACR > Security > Secure Student Administration > User ID > Data Security Summary** to see a full picture of a user’s data security. Enter the user’s HUID in the search bar and click **Search**.



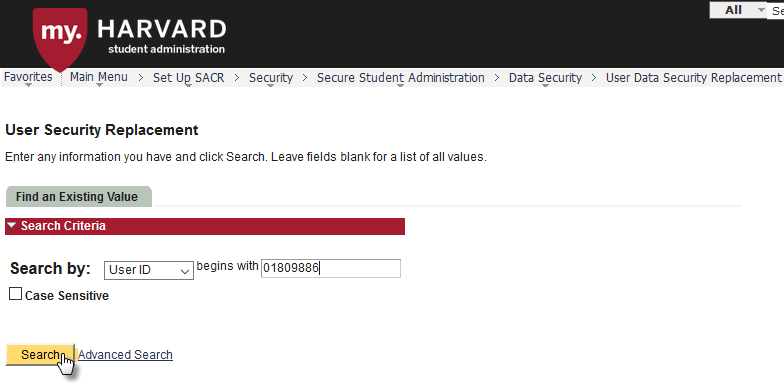
The user’s data security summary will appear. Multiple tabs cover the different data security categories. This page also show which committees the user is assigned to and any FTP security he or she may have. Click on the arrow next to Data Security Summary 3 to see the other tabs. You can also see the full list of the tabs at the bottom of the page.



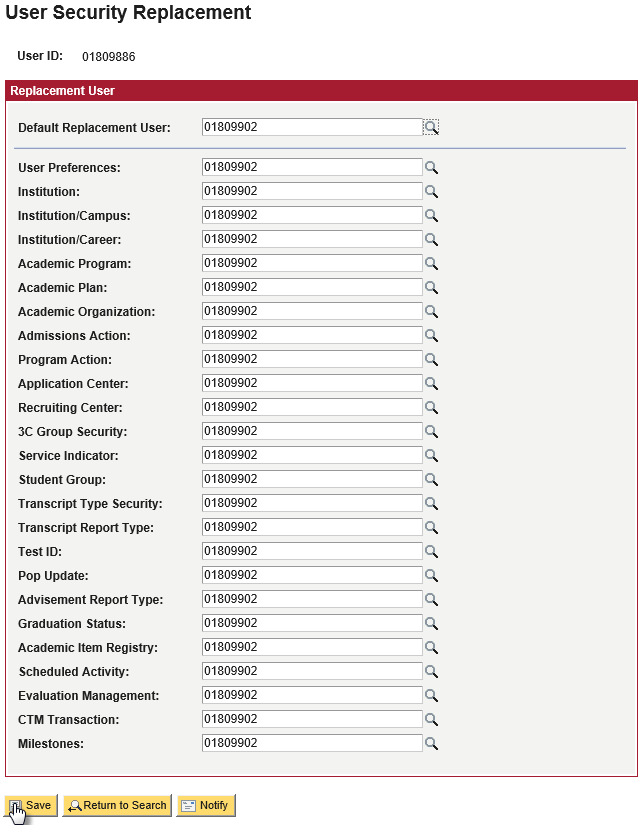
On the home page, navigate to the Security Pagelet. Under the **Data Security Links** tab, click on **Data Security Replacement**.



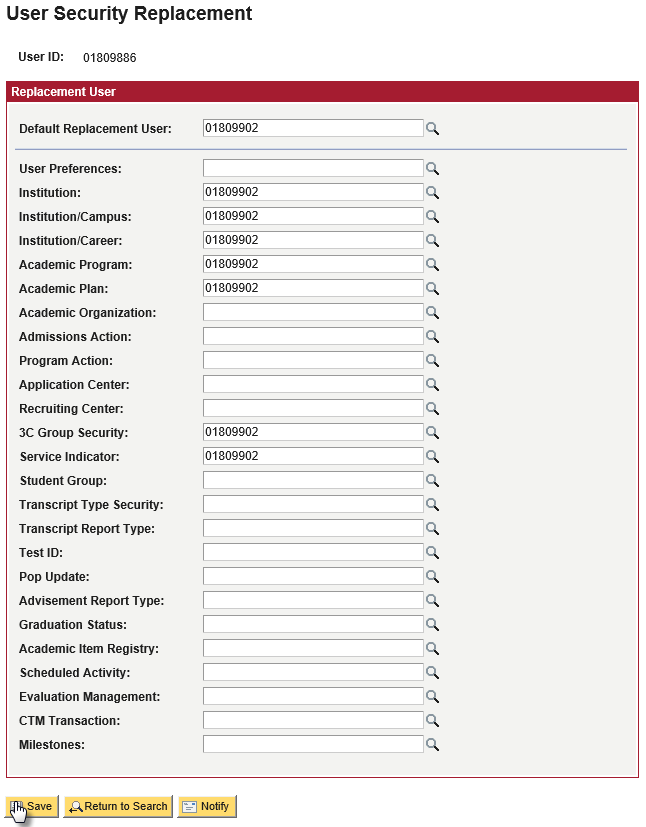
A new window will open up to the User Security Replacement page. Enter the user’s HUID in the search bar and click **Search**.



Now enter the HUID of the data security you want to copy, and click on the tab key. This will populate all of the categories. Click **Save** if you wish to copy all the data security categories.



If you wish to only copy one or a few data security categories, simply just enter the HUID in those search bars (there is no need to enter it in the Default Replacement User search bar). Click **Save** to save the changes.



## Transfer User Process

There is no automated process for transfers. The expectation is that departments within the schools and/or the schools’ registrar’s office will communicate any such transfers through a Service Now ticket and provide instructions on what access should be retained.

# Access Roles

## Role Modifications / New Roles

Access role modifications or new roles should come from the Local Security Administrators. There may be exceptions such as the user is a super user within the school such as a member of the Registrar Office. However, role modifications should not be made lightly as granting out too much access could have adverse effects on the system or result in data not being secured appropriately. To request or modify access for a role, send an email [sis\_security@harvard.edu](mailto:sis_security@harvard.edu) with the following information: the role(s), the page(s) that need to be added or modified, access to these pages (add, update, display, correct), and why this access is needed.

# Non Production Environments

In addition to the production admin and portal sites there are the following non production environments found in **nonprod.my.harvard.edu**:

|  |  |  |
| --- | --- | --- |
| **Environment** | **Campus Solutions (Admin)** | **Interactive HUB (Portal)** |
| TST | CS TST | ENT PORTAL TST |
| INT | CS INT | ENT PORTAL INT |
| Production 2 | CS PR2 | ENT PORTAL PR2 |