Channel Islands
CALIFORNIA STATE UNIVERSITY

CI Records Automated PSAR

Process Guide

Last Revised: **9/10/2014**

REVISION CONTROL

Document Title: CI Records Automated PSAR– Process Guide

Author: Shawn Bochat –Technology & Communication

File Reference: CI Records Automated PSAR- Process Guide - 2014.09.10.docx

Date	By	Action	Pages
7/1/2014	Shawn Bochat	Creation of Document	All

Review/Approval History

Date	By	Action	Pages
7/10/2014	Shawn Bochat	Initial Draft	All
8/4/2014	Shawn Bochat	Finalized Draft	All
9/10/2014	Shawn Bochat	Finalized Draft- Review	All

Table of Contents

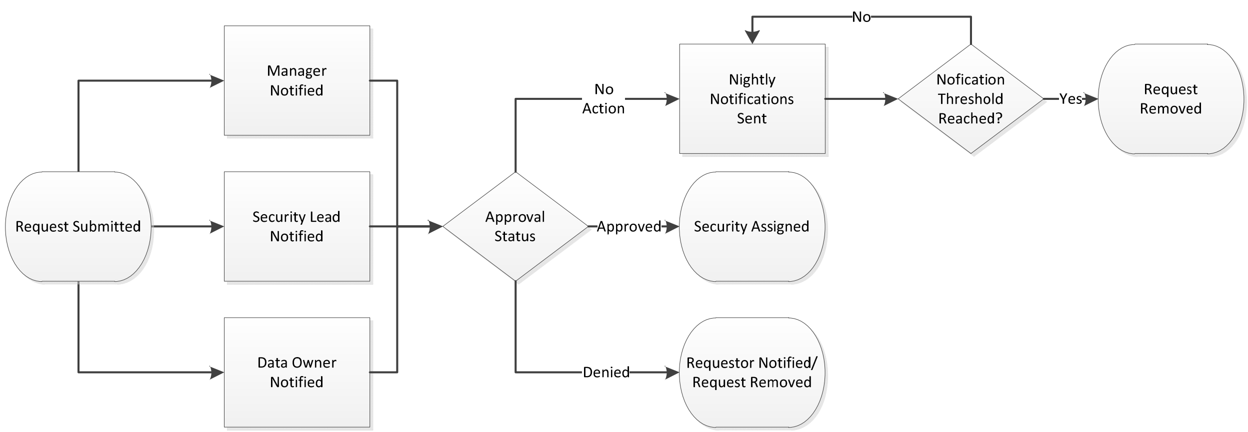
1.0 Purpose

The PSAR (PeopleSoft Security Access Request) Process Guide outlines the functionality of the CI_PT_SC_0003 modification. This includes pages to request, approve, and remove Channel Islands defined PeopleSoft security roles. Additionally this process guide provides details about the processes, configuration, notifications and workflow included in the project.

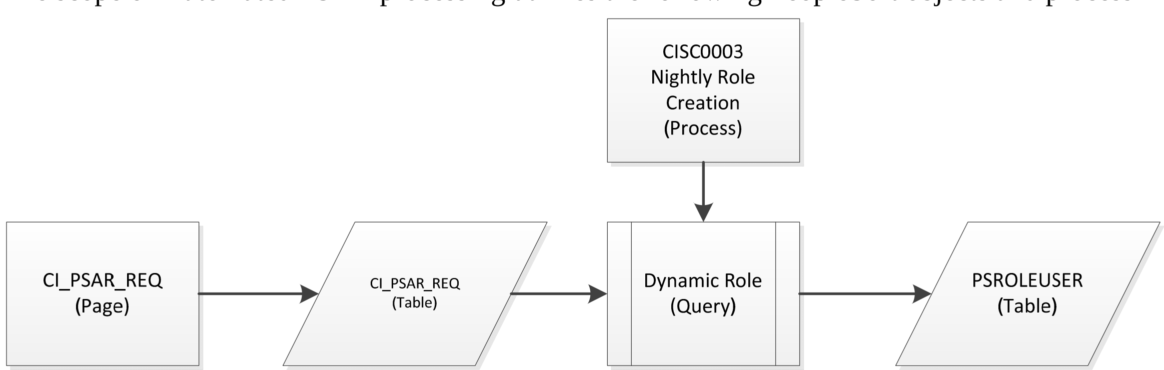
2.0 Overview

This document will provide an overview of the Channel Islands Automated PeopleSoft System Access Request modification. This modification includes PeopleSoft Page based components for the requesting and approval of PeopleSoft security, as well as Page based components for review and removal of PeopleSoft security. Workflow notifications are handled through campus email (using the employee domain addresses configured in PeopleSoft) and occur at the time of a request as well as nightly based on configuration thresholds. Assignment of security in PeopleSoft delivered components is predicated off of the transactions entered, approved, or removed in the PSAR request pages. Security assignment occurs 3 times each business day. The Automated PSAR project also provides process-based functionality for creating dynamic role queries, mass notification and automated removal of denied/expired requests.

The following represents the process flow for new PSAR transactions:



The scope of Automated PSAR processing utilizes the following PeopleSoft objects and process flow:



2.1 Roles & Responsibilities

Requester – A requestor is defined as a CI Records user, who initiates individual PSAR transactions. Requestors may also fulfill any of the other roles outlined in this section based on their relationship to the campus. Requestors are responsible for determining and/or coordinating an appropriate link between CI Records users requiring new access and the roles containing that access, during the request submission process.

***MPP Manager* -** Manager is defined as an individual whose responsibility is assigning and managing administrative and operational duties. This individual is classified as Management Personnel in HR (MPP). Managers are responsible for approving PSAR requests on behalf of appropriate employees.

Security Lead – Security Lead is defined as an individual who has been delegated by a Data Owner as the individual responsible for the creation, review, request and approval of the various PeopleSoft security components (including but not limited to profiles, roles, permission lists, and query security). Security Leads are responsible for approving PSAR requests that contain the security components delegated as their responsibility.

***Data Owner* -** Data Owner (also known as Data Steward) is defined as an individual who has been delegated with the following responsibilities within their delegated area of ownership/stewardship:

1. Classification of information assets according to the campus Data Classification Standard.
2. Define security requirements proportionate to the value of information assets within delegated area.
3. Management of delegated information assets according to the requirements described in the campus Information Asset Management Standard and the CSU Records Retention Schedule for their delegated area.

Data Owners are responsible for approving requests that contain data and/or components under their stewardship.

Approver – An approver is a general term for anyone who fulfills the role of a MPP Manager, Security Lead, and/or Data Owner for the campus.

2.2 Security Considerations

This section lists all security considerations for the process

Page Security – Appropriate page security will be required to access the request and configuration pages. One set of security will be created for PSAR approvers to make and approve request, another will be created for the Campus PeopleSoft Security Administrator(s).

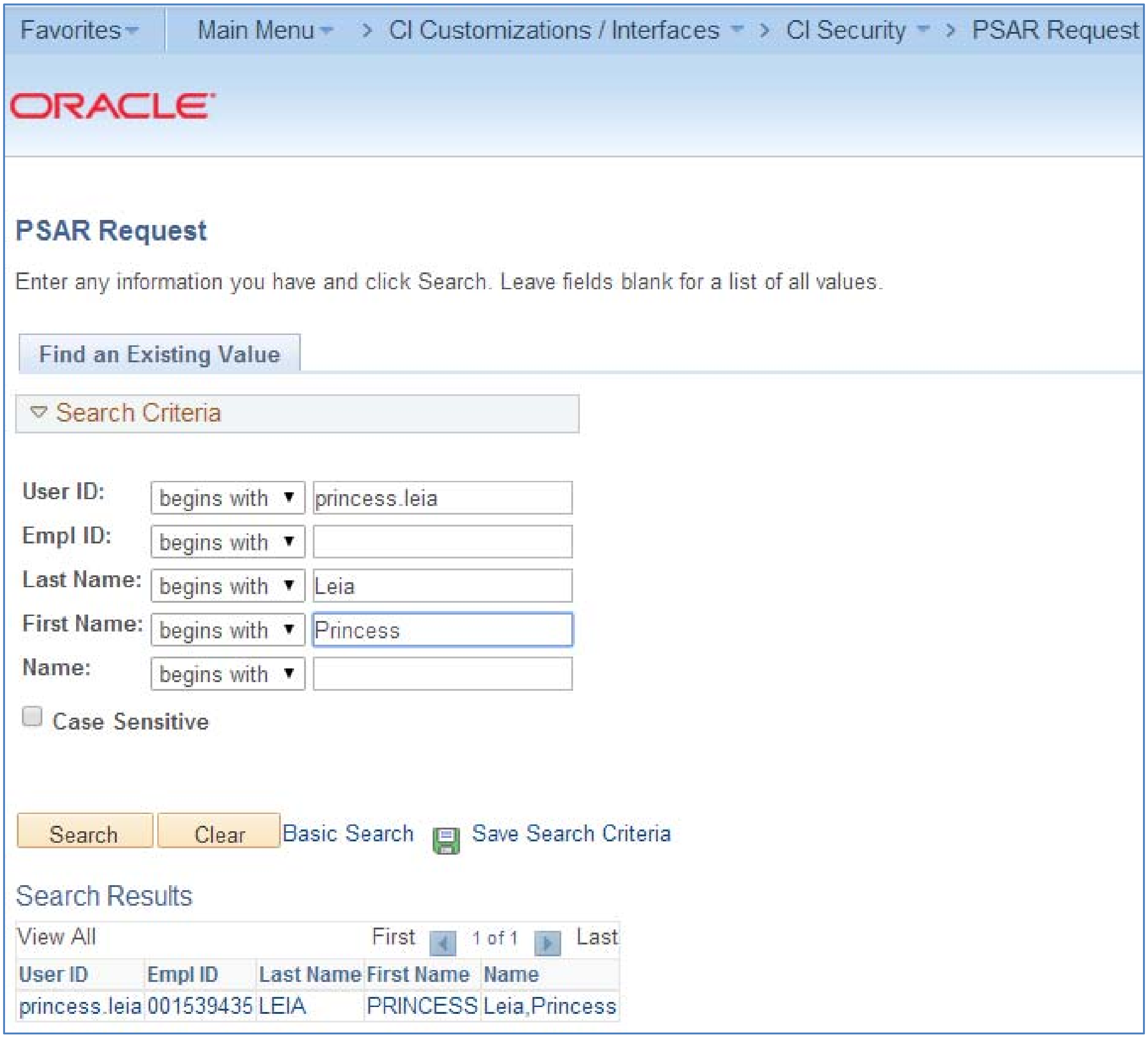
Process Security – Appropriate process security will be required to run the processes.

3.0 PSAR Requests and Approvals

This section will walk through the process of making and approving a PSAR request in CI Records. PSAR requests and their associated approvals drive the assignment of CI Records security. Fully approved requests are translated into security assignments **three** times each business day.

3.1 Creating a PSAR Request

Navigation: Main Menu > CI Customization / Interfaces > CI Security > PSAR Request

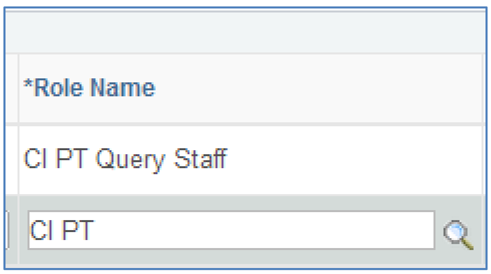


1. **Enter** in search criteria at the Find an Existing Value
2. **Click** Search 

3. **Select** the Employee from the Search Results section if prompted

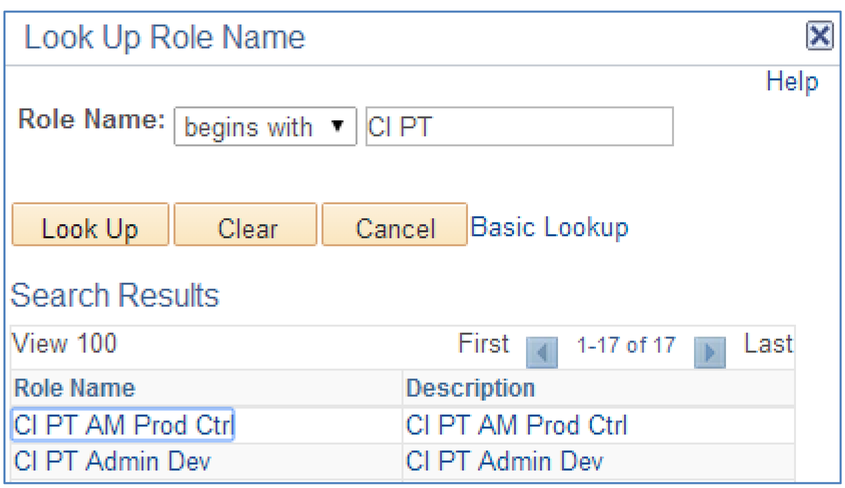
> Note: Only campus employees who have a CMS Compliance Form on file will appear in the search results. The CMS Compliance Form is provided by Human Resources during the hiring process and requires both the employees and appropriate manager's signature. More information can be found here: http://www.csuci.edu/hr/hr_documents/cms-complianceaccess-form-oct2012.pdf

4. **Click** the add a row icon



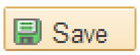
5. **Enter** all or some of the Role Name in the Role Name field, if possible. Otherwise proceed to the next step.

6. **Click** the search icon on the Role Name column



7. **Click** the Role Name you would like to request

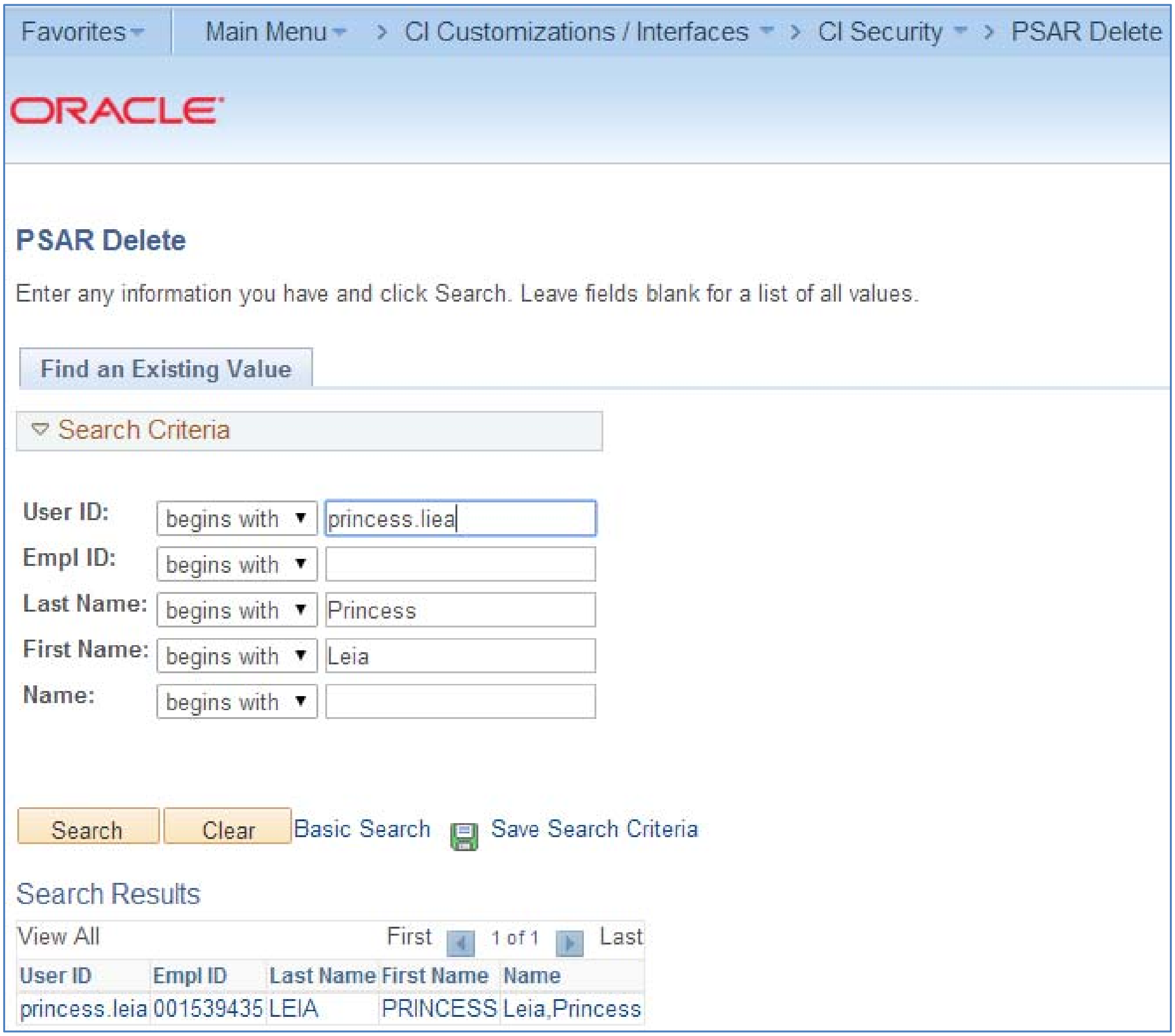

PSAR Request
Empl ID 001539435 Leia,Princess
User ID princess.leia
Personalize | Find | View All |
First 1-3 of 3 Last
PS System
*Role Name
*MPP Approved
MPP
*Data Owner Approved
Data Owner
*Security Lead Approved
Security Lead
Request Date/Time
1 HCM CI PT Query Staff Pending Solo,Han Pending Skywalker,Luke Pending Skywalker,Luke 07/18/14 12:41PM
2 HCM CI PT Sec SF Row Pending Solo,Han Pending Skywalker,Luke Pending Skywalker,Luke 07/12/14 8:12PM
3 HCM CI PT Security Lead Requesting Solo,Han Requesting Skywalker,Luke Requesting Skywalker,Luke 08/06/14 2:51PM
Role Definitions
Save
Return to Search
Notify

8. **Click** Save 
Save

3.2 Deleting a PSAR Request

Deletion of PSAR request results in either the prevention of CI Records assignment (if the request is not yet fully approved) or the removal of existing CI Records security.

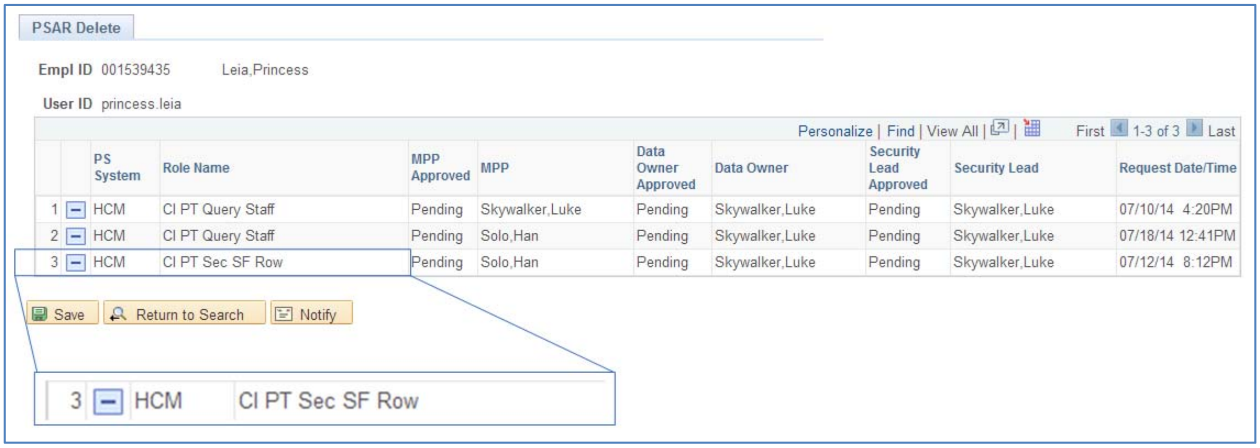
Navigation: Main Menu > CI Customization / Interfaces > CI Security > PSAR Delete



1. **Enter** in search criteria at the Find an Existing Value
2. **Click** Search 

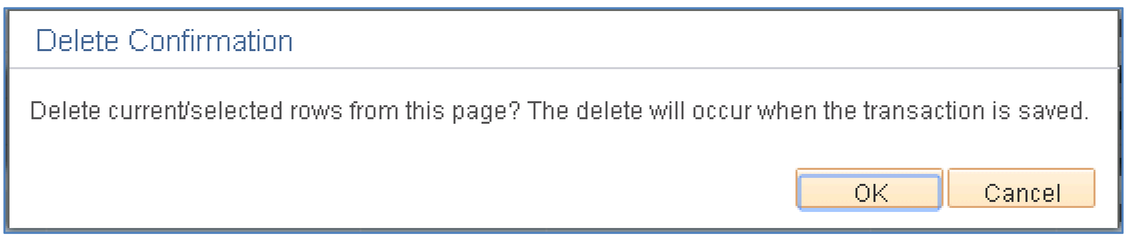
3. **Select** the Employee from the Search Results section if provided the option

Note: Only campus employees who have a CMS Compliance Form on file appear in the search results. The CMS Compliance Form is provided by Human Resources during the hiring process and requires both the employees and appropriate manager's signature. More information can be found here: http://www.csuci.edu/hr/hr_documents/cms-complianceaccess-form-oct2012.pdf



	PS System	Role Name	MPP Approved	MPP	Data Owner Approved	Data Owner	Security Lead Approved	Security Lead	Request Date/Time
1	HCM	CI PT Query Staff	Pending	Skywalker,Luke	Pending	Skywalker,Luke	Pending	Skywalker,Luke	07/10/14 4:20PM
2	HCM	CI PT Query Staff	Pending	Solo,Han	Pending	Skywalker,Luke	Pending	Skywalker,Luke	07/18/14 12:41PM
3	HCM	CI PT Sec SF Row	Pending	Solo,Han	Pending	Skywalker,Luke	Pending	Skywalker,Luke	07/12/14 8:12PM

4. **Click** Remove  icon next to the role you want removed.



5. **Click** OK  when the dialog box appears.

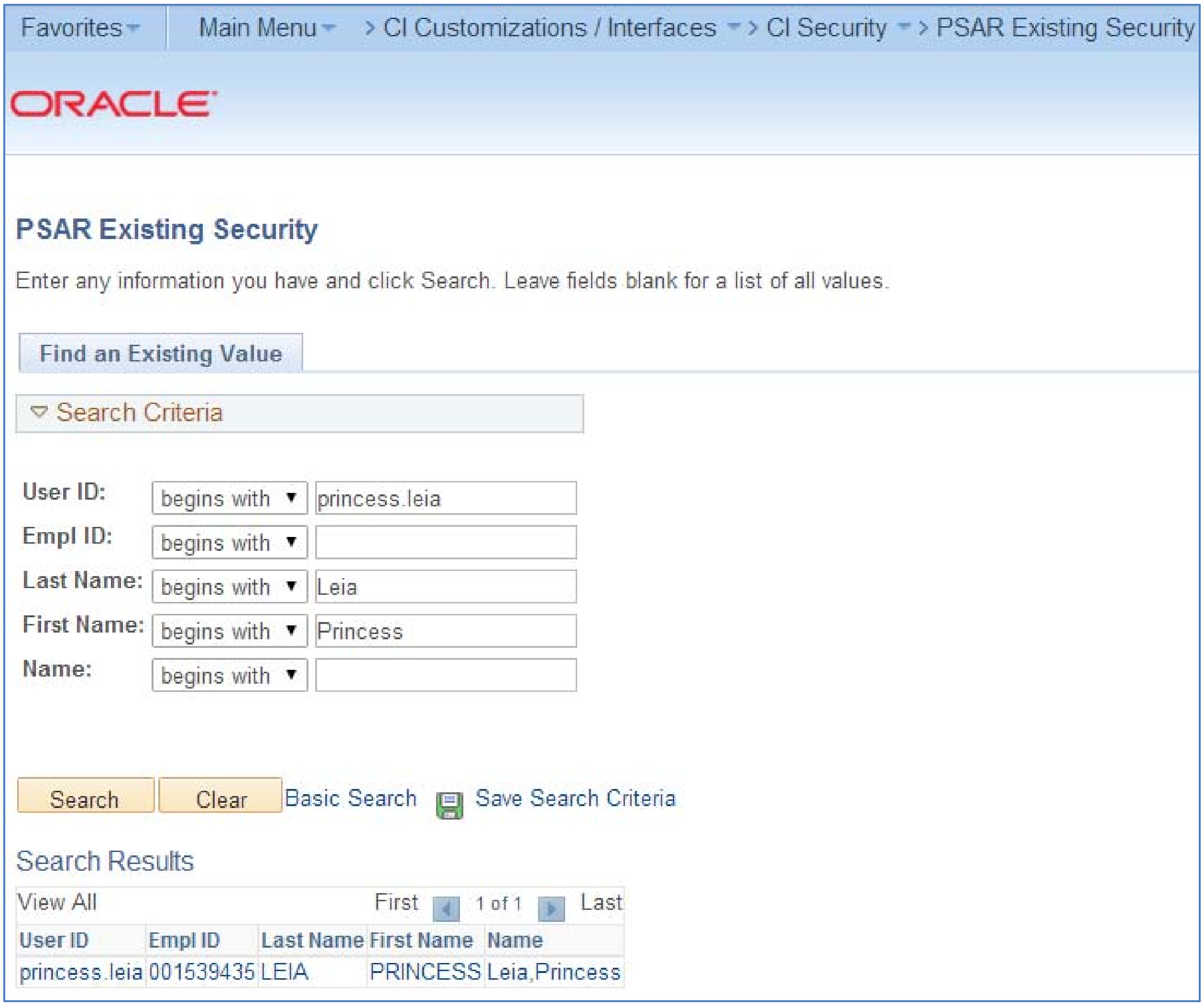
	PS System	Role Name	MPP Approved	MPP	Data Owner Approved	Data Owner	Security Lead Approved	Security Lead	Request Date/Time
1	HCM	CI PT Query Staff	Pending	Skywalker,Luke	Pending	Skywalker,Luke	Pending	Skywalker,Luke	07/10/14 4:20PM
2	HCM	CI PT Query Staff	Pending	Solo,Han	Pending	Skywalker,Luke	Pending	Skywalker,Luke	07/18/14 12:41PM

6. **Click** Save  when you are returned to the page and have finished removing requests.

3.3 View Existing Security

Viewing existing security provides a full picture of users with CI Records existing security.

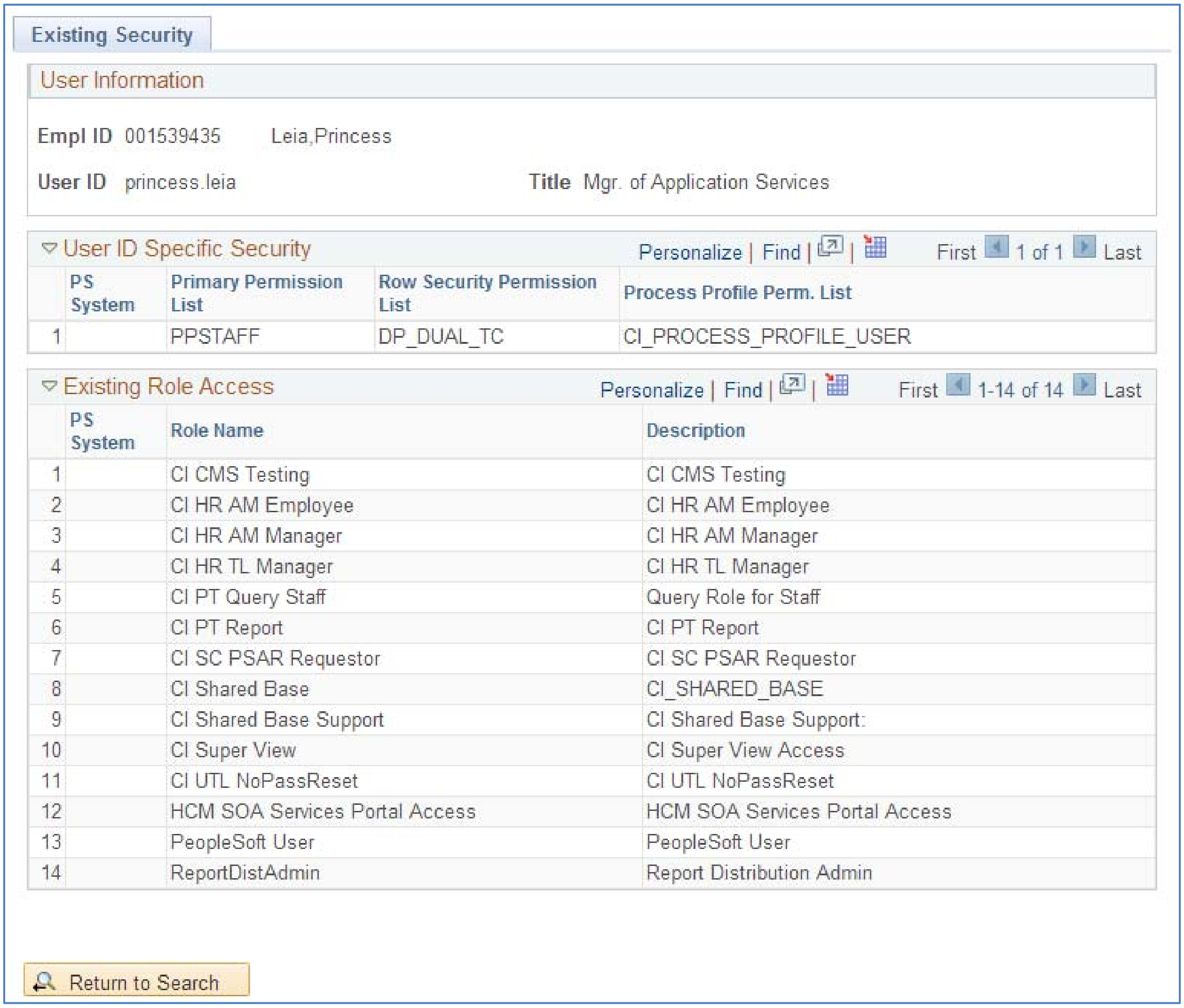
Navigation: Main Menu > CI Customization / Interfaces > CI Security > PSAR Existing Security



1. **Enter** in search criteria at the Find an Existing Value
2. **Click** Search 

3. **Select** the Employee from the Search Results section if provided the option

> Note: Only campus employees who have a CMS Compliance Form on file appear in the search results. The CMS Compliance Form is provided by Human Resources during the hiring process and requires both the employees and appropriate manager's signature. More information can be found here: http://www.csuci.edu/hr/hr_documents/cms-complianceaccess-form-oct2012.pdf



Existing Security

User Information

Empl ID 001539435 Leia,Princess

User ID princess.leia **Title** Mgr. of Application Services

User ID Specific Security — Personalize | Find | | First 1 of 1 Last

	PS System	Primary Permission List	Row Security Permission List	Process Profile Perm. List
1		PPSTAFF	DP_DUAL_TC	CI_PROCESS_PROFILE_USER

Existing Role Access — Personalize | Find | | First 1-14 of 14 Last

	PS System	Role Name	Description
1		CI CMS Testing	CI CMS Testing
2		CI HR AM Employee	CI HR AM Employee
3		CI HR AM Manager	CI HR AM Manager
4		CI HR TL Manager	CI HR TL Manager
5		CI PT Query Staff	Query Role for Staff
6		CI PT Report	CI PT Report
7		CI SC PSAR Requestor	CI SC PSAR Requestor
8		CI Shared Base	CI_SHARED_BASE
9		CI Shared Base Support	CI Shared Base Support:
10		CI Super View	CI Super View Access
11		CI UTL NoPassReset	CI UTL NoPassReset
12		HCM SOA Services Portal Access	HCM SOA Services Portal Access
13		PeopleSoft User	PeopleSoft User
14		ReportDistAdmin	Report Distribution Admin

Return to Search

4.0 PSAR Notifications

The CI Records PSAR Automation project provides an approval workflow framework using campus email addresses. These notifications are triggered by the CI Records PSAR request page (section 3.1) and the scheduled nightly processes. This section will explain the types of notifications generated by the Automated PSAR modification and when they are sent.

4.1 New PeopleSoft System Access Requests for...

New system PSAR requests require three levels of approval: MPP Manager of the employee, Security Lead associated to the role, and Data Owner associated to the role. For typical Automated PSAR requests, the requester does not fulfill each of these roles. Therefore at the time of request submission (see Section 3.1) an email is sent directly to each approver who does fulfill any of the three roles the requestor does not. There is no order precedence for approval for PSAR requests; therefore emails go out to all approvers who have pending action on the request immediately.

The subject of a New PeopleSoft System Access Requests email will indicate to the approver that a new request for a particular employee requires their attention. The body of the email contains: the name of the requestor, the date of the request, the name of the employee for whom the security is being requested, the emplid of the employee for whom the security is being requested, the role being requested for the employee, and a link into CI Records where the request can be approved (MyCI login may be necessary).

Subject: New PeopleSoft System Access Request for Princess Leia

A PeopleSoft System Access Request was created by Luke Skywalker on 2014-07-19. The request consists of:

Name: Princess Leia
Emplid: 001539435
Role: CI PT Sec SF Row

Please provide approval at:
https://cmsdev3.calstate.edu/psp/HACITST/EMPLOYEE/HRMS/c/CI_SC_CUSTOM.CI_PSAR_REQ.GBL?Page=CI_PSAR_REQ&Action=U&EMPLID=001539435

4.2 PeopleSoft System Access Request Denied for …

If an approver should determine that an Automated PSAR request cannot be approved, they have the ability to deny approval on the PSAR request page. When a request is denied an email is sent to the original requester.

The PeopleSoft System Access Denial email subject indicates to the requester that a request they submitted on behalf of a particular employee has been denied. The body of the email contains the name of the approver who denied the request, the employee name, the employee ID, the role requested, and the date of the original request.

Subject: PeopleSoft System Access Request Denied for Princess Leia

Han Solo has denied the following PeopleSoft System Access Request:

Employee: Princess Leia
Emplid: 999000999
Role: CI AA Faculty Pgrm Adv Staff
Submitted: 2014-07-14

Denied requests are removed nightly.

Note: Denied requests are purged nightly. If you receive a denial notification and feel it is in error – **contact the approver immediately**. The approver can change their approval status within the same business day.

4.3 PeopleSoft System Access Reminder

When outstanding PSAR requests are left in a pending status by approvers, CI Records security is not assigned. Likewise, the Automated PSAR modification only sends one initial notice to approvers for each unique PSAR request. As a reminder to approvers who have unaddressed and outstanding requests that require attention, the Automated PSAR modification sends out nightly reminder emails. Configuration for the modification includes a threshold value for outstanding requests. When an approver has one or more outstanding requests that have passed the threshold the PSAR modification begins sending the nightly reminder emails.

The PeopleSoft System Access Requests Reminder email subject notifies approvers that they have request requiring attention. The threshold value and outstanding requests for each function the approver servers are include in the body of the email. The employee name, employee ID, role name, and original request date of each outstanding request are also included.

Subject: PeopleSoft System Access Request Reminder

The following CI Records PSAR requests have been pending your review for 7 days or longer.

MPP Mangager requests outstanding:
EMPLOYEE: Princess Leia (001539435), ROLE: CI PT Query Staff, REQUEST DATE: 10-07-2014

Data Owner requests outstanding:
EMPLOYEE: Princess Leia (001539435), ROLE: CI PT Query Staff, REQUEST DATE: 10-07-2014
EMPLOYEE: Princess Leia (001539435), ROLE: CI PT Sec SF Row, REQUEST DATE: 12-07-2014

Security Lead requests outstanding:
EMPLOYEE: Princess Leia (001539435), ROLE: CI PT Query Staff, REQUEST DATE: 10-07-2014
EMPLOYEE: Princess Leia (001539435), ROLE: CI PT Sec SF Row, REQUEST DATE: 12-07-2014

4.4 PeopleSoft System Access Request Expiration

Similar to the reminder threshold described in the previous section, the Automatic PSAR modification has an expiration threshold. If an approver has not addressed outstanding requests by the threshold days after the original request date, a PSAR request is removed from CI Records and the original requester is notified.

The PeopleSoft System Access Request Expiration notification includes a descriptive subject and the fields describing each expiring request including: the employee name, employee ID, role name, request date, mpp manager name, mpp manager approval status, data owner name, data owner approval status, security lead name, and security lead status.

Subject: PeopleSoft System Access Request Expiration

The following CI Records PSAR request(s) have not been approved in the maximum 14 days:
EMPLOYEE: Princess Leia (999000000)
ROLE: CI SR Health Center Staff
REQUEST DATE: 03-07-2014
MANAGER: Luke Skywalker STATUS: A
DATA OWNER: Darth Vader STATUS: P
SECURITY LEAD: Bobba Fett STATUS: P

EMPLOYEE: Princess Leia (999000000)
ROLE: CI HR TL Manager
REQUEST DATE: 03-07-2014
MANAGER: Luke Skywalker STATUS: A
DATA OWNER: Han Solo STATUS: P
SECURITY LEAD: Chewbacca STATUS: P

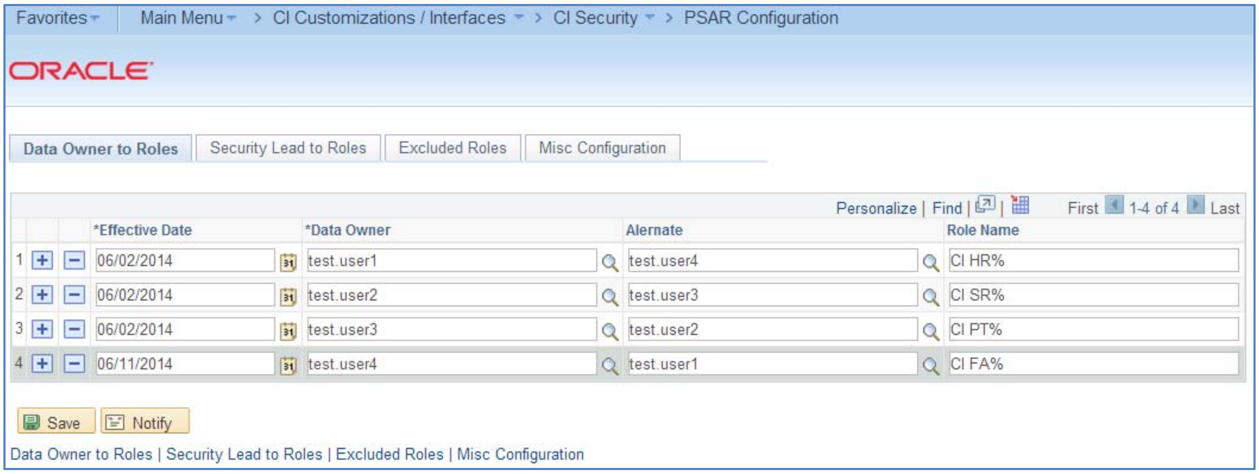
5.0 PSAR Configuration

This section will walk through the process of configuring the Automatic PSAR modification. Each section outlined is crucial for the effective operation of the Automate PSAR modification. Data Owner and Security Lead associations to roles enable the notification and approval structure of the modification. The Excluded Roles component allows Data Owners and Security Leads to opt out certain roles of the Automated PSAR request process. Finally, the Misc Configuration tab handles the setup and storage of all other modification required values.

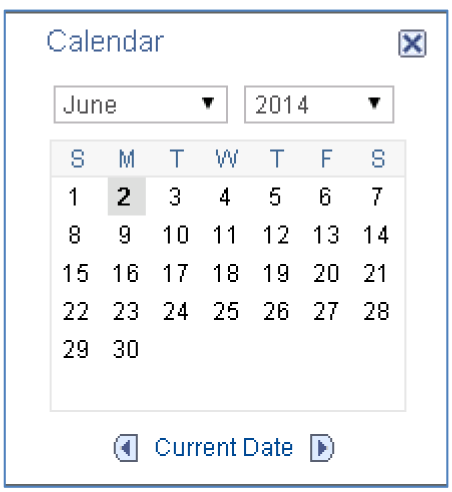
5.1 Define Data Owners to Role Relationships

Navigation: CI Customization / Interfaces > CI Security > PSAR Configuration > Data Owner to Roles (tab)

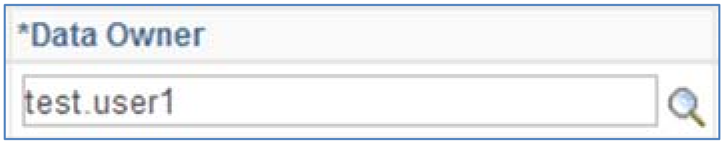
This page links subsets of custom CI security roles to the appropriate Data Owners. Roles are grouped by using the campus role naming convention and a wild card operator '%'. Alternate approvers can be configured and the assignments adhere to effective dated logic.



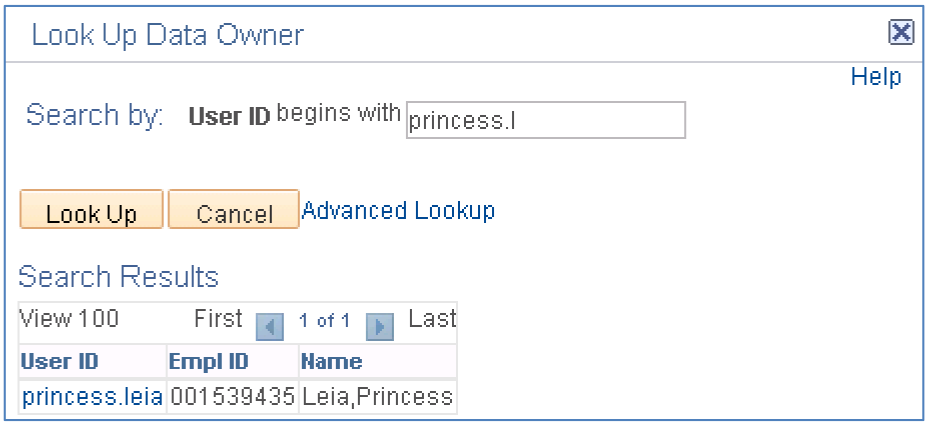
1. **Add** a new row.



2. **Enter** an Effective Date (or continue with the default value).

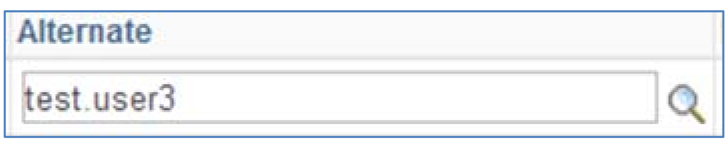


3. **Enter** a Data Owner's User ID and skip the next two steps, or **click** search 

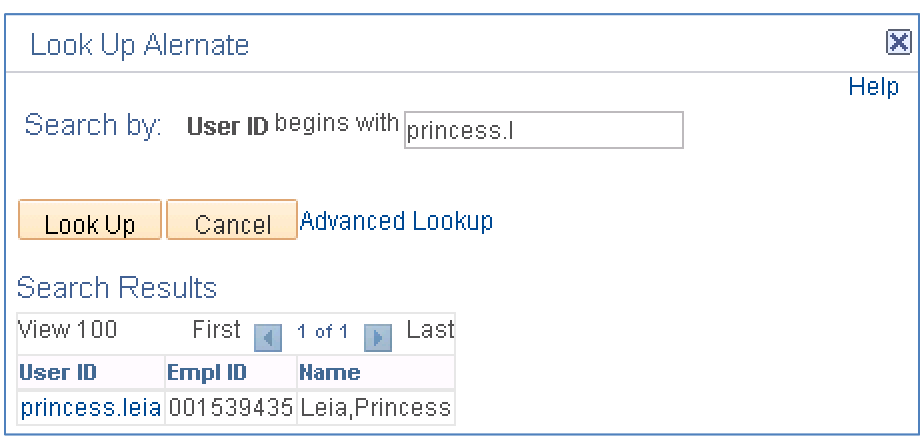


4. **Enter** a Data Owner's User ID, the Look Up button  will bring up a listing of all matching values (or all values if the field is left blank)

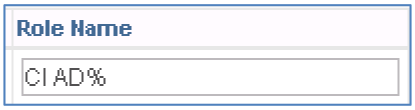
5. **Click** the User ID of the Data Owner.



6. If requested by the Data Owner, **Enter** an Alternate User ID and skip the next two steps, or **click** search 



7. **Enter** an Alternate's User ID, the Look Up button  will bring up a listing of all matching values (or all values if the field is left blank)
8. **Click** the User ID of the Alternate.



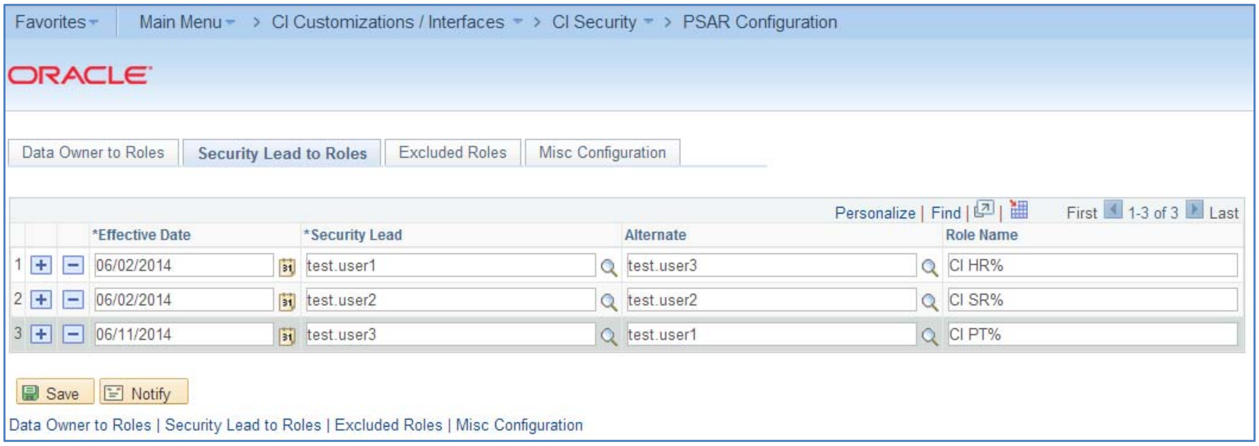
9. **Enter** as role name descriptor, with the '%' wild card symbol if needed

10. **Click** Save 

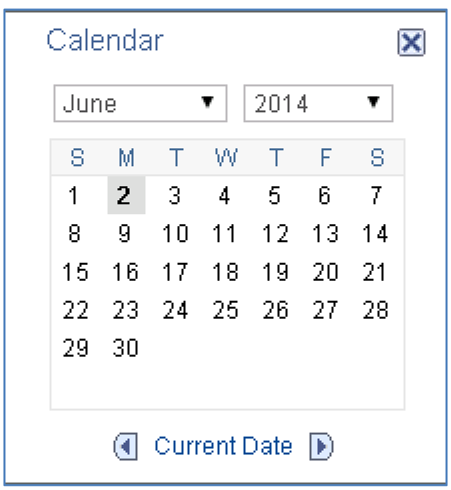
5.2 Define Security Leads to Role Relationships

Navigation: CI Customization / Interfaces > CI Security > PSAR Configuration > Security Lead to Roles (tab)

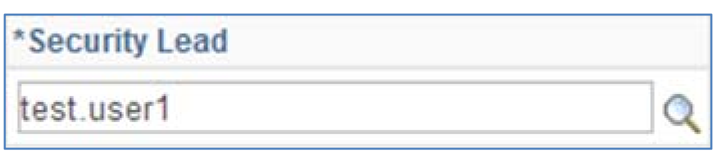
This page links subsets of custom CI security roles to the appropriate Security Lead. Roles are grouped by using the campus role naming convention and a wild card operator '%'. Alternate approvers can be configured and the assignments adhere to effective dated logic.



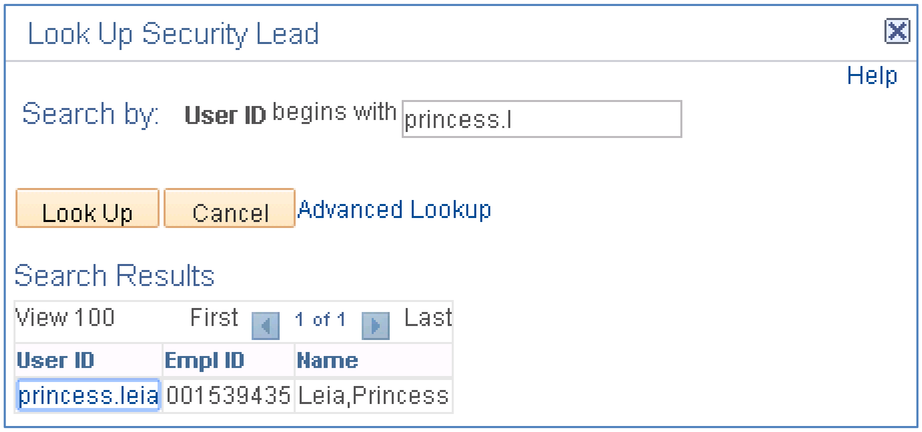
1. **Add** a new row.



2. **Enter** an Effective Date (or continue with the default value).

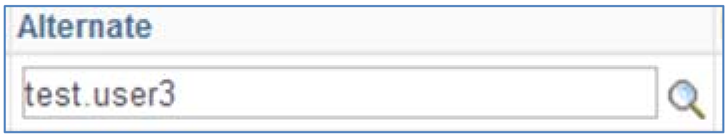


3. **Enter** a Security Leads User ID and skip the next two steps, or **click** search

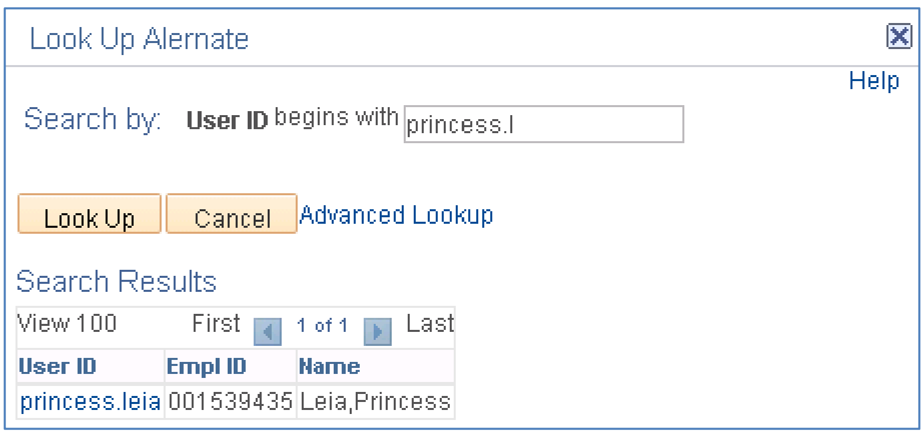


4. **Enter** a Security Lead's operator ID, the Look Up button  will bring up a listing of all matching values (or all values if the field is left blank)

5. **Click** the User ID of the Security Lead.

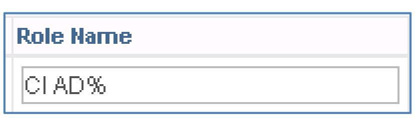


6. If requested by the Security Lead, **Enter** an Alternate User ID and skip the next two steps, or **click** search 



7. **Enter** an Alternate's operator ID, the Look Up button  will bring up a listing of all matching values (or all values if the field is left blank)

8. **Click** the User ID of the Alternate.

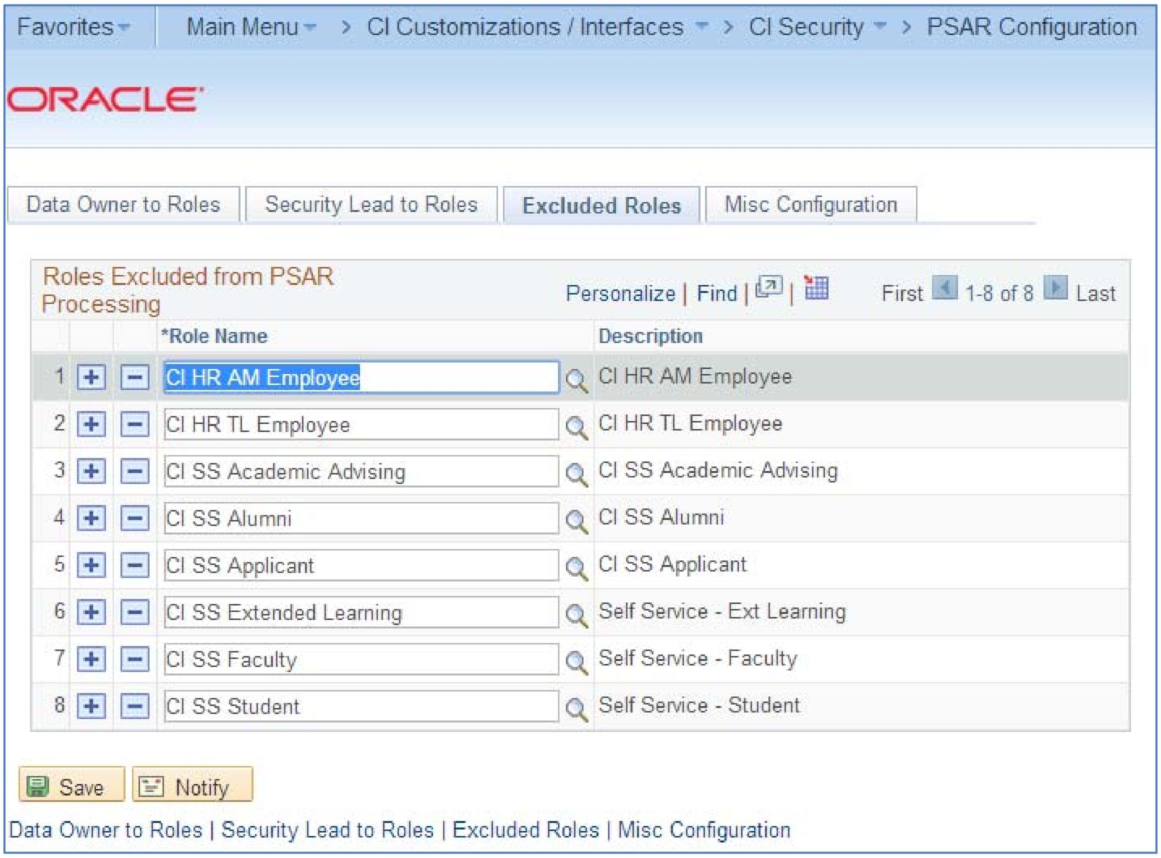


9. **Enter** as role name descriptor, with the '%' wild card symbol where needed
10. **Click** Save 

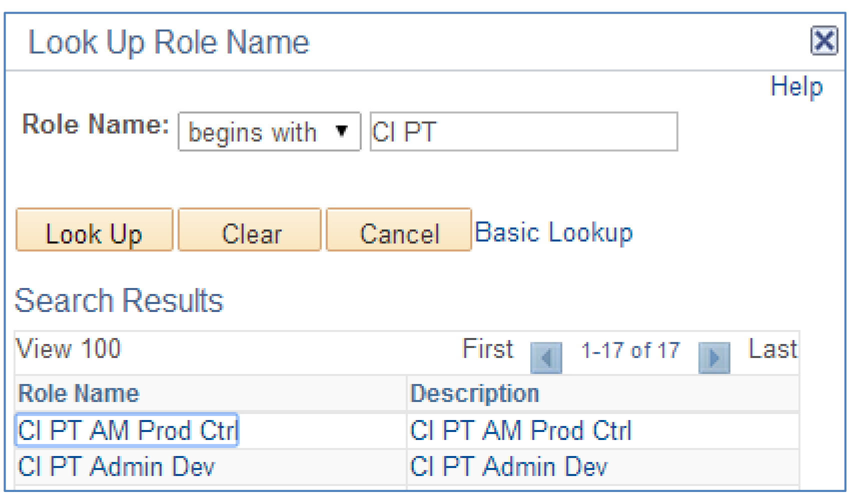
5.3 Define Roles Excluded from PSAR Processing

Navigation: CI Customization / Interfaces > CI Security > PSAR Configuration > Excluded Roles (tab)

This page lists roles that need to be excluded from automatic PSAR processing.



1.  **Add** a new row.



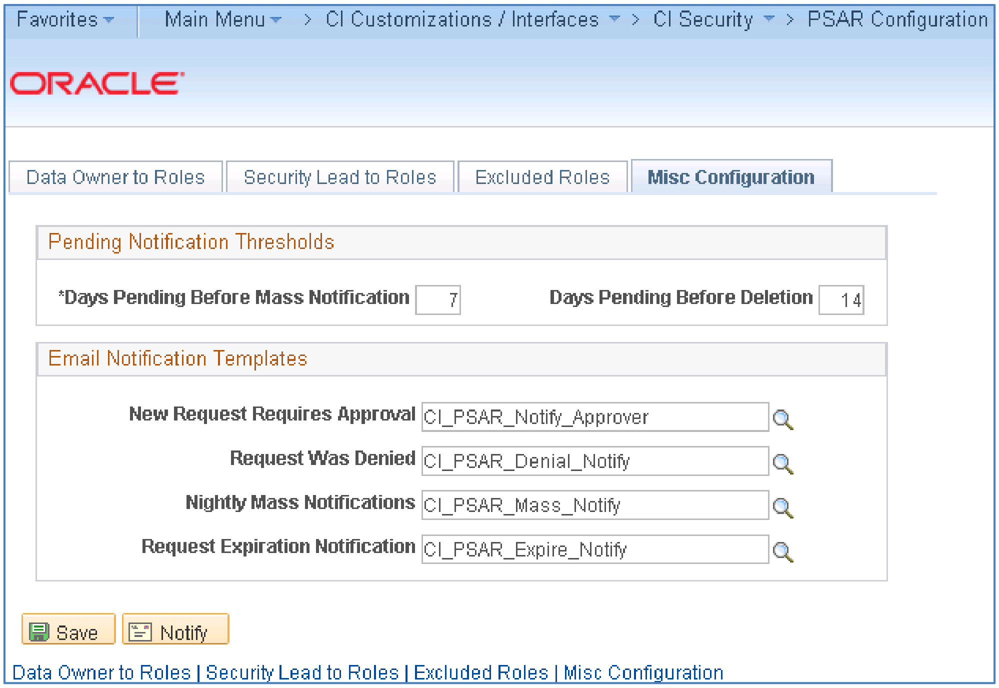
2. **Search** and select a Role Name in dialog box

3. **Click** Save 

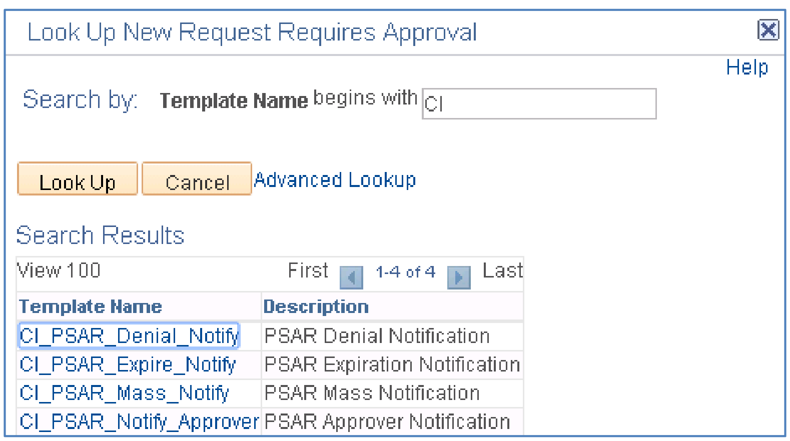
5.4 Define Miscellaneous Configuration from PSAR Processing

Navigation: CI Customization / Interfaces > CI Security > PSAR Configuration > Misc Configuration (tab)

This page defines several required configuration values for the PSAR modifications. These include workflow notification thresholds and email notification Templates.



1. **Enter** an Integer value for the *Days Pending Before Mass Notification* field
2. **Enter** an Integer value for the *Days Pending Before Deletion* field



3. **Search** and **Select** a template for *New Request Requires Approval*
4. **Search** and **Select** a template for *Request Was Denied*
5. **Search** and **Select** a template for *Nightly Mass Notifications*
6. **Search** and **Select** a template for *Request Expiration Notification*
7. **Click** Save

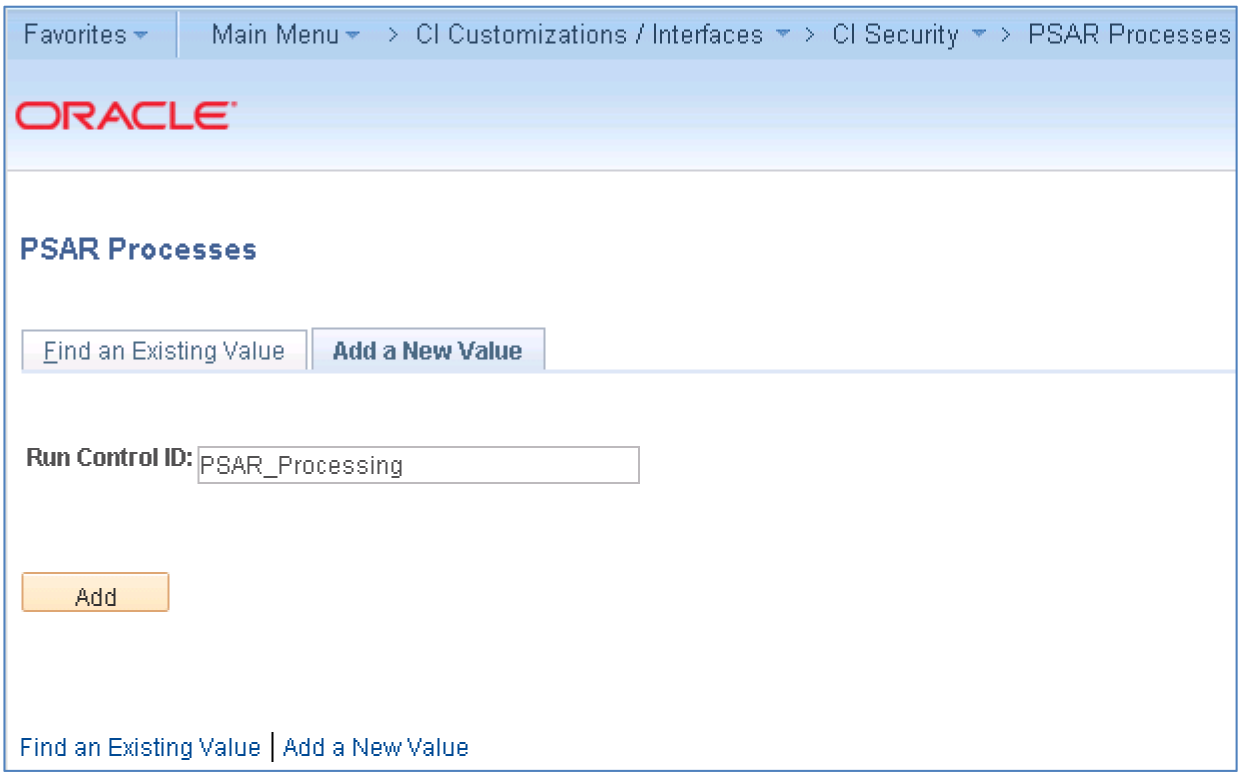
6.0 PSAR Processes

This section will walk through running the two processes included in the Automated PSAR modification. The CISC0003 SQR Process creates dynamic role queries for appropriate CI Records security roles – it is a Scheduled process run nightly by the system and not a user run process. The CISC0003 Application Engine process sends notification emails for unaddressed PSAR requests and removes denied requests – it is a Scheduled process run nightly by the system and not a user run process.

6.1 Define a Run Control – (One Time Step)

This step is only done once, subsequent process runs can be started at section 6.2.

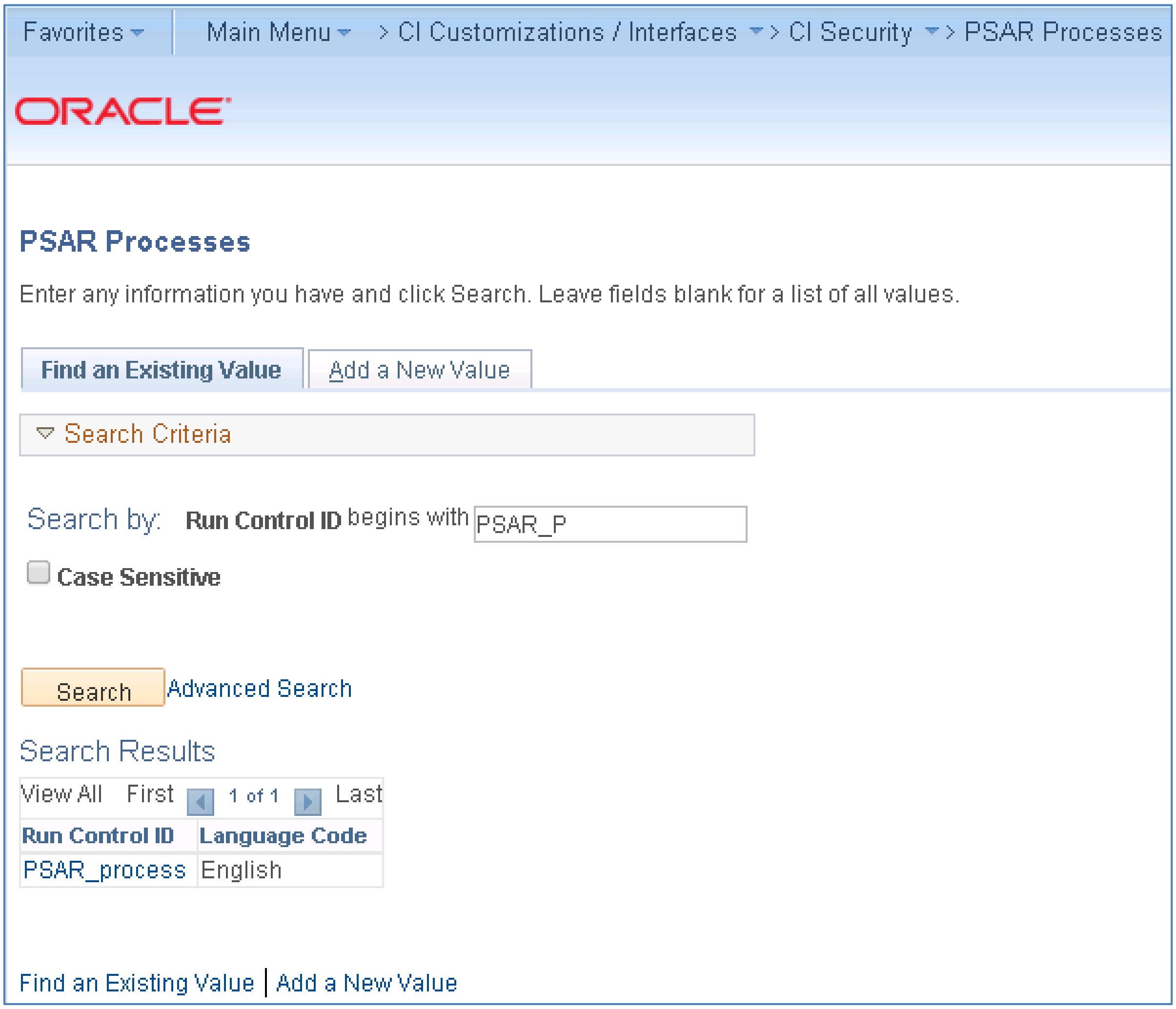
Navigation: CI Customization / Interfaces > CI Security > PSAR Processes > Add a New Value (tab)



1. **Select** the Add a New Value upon your first visit to the Page
2. **Enter** a Run Control ID
3. **Click** Add

6.2 Open an existing Run Control

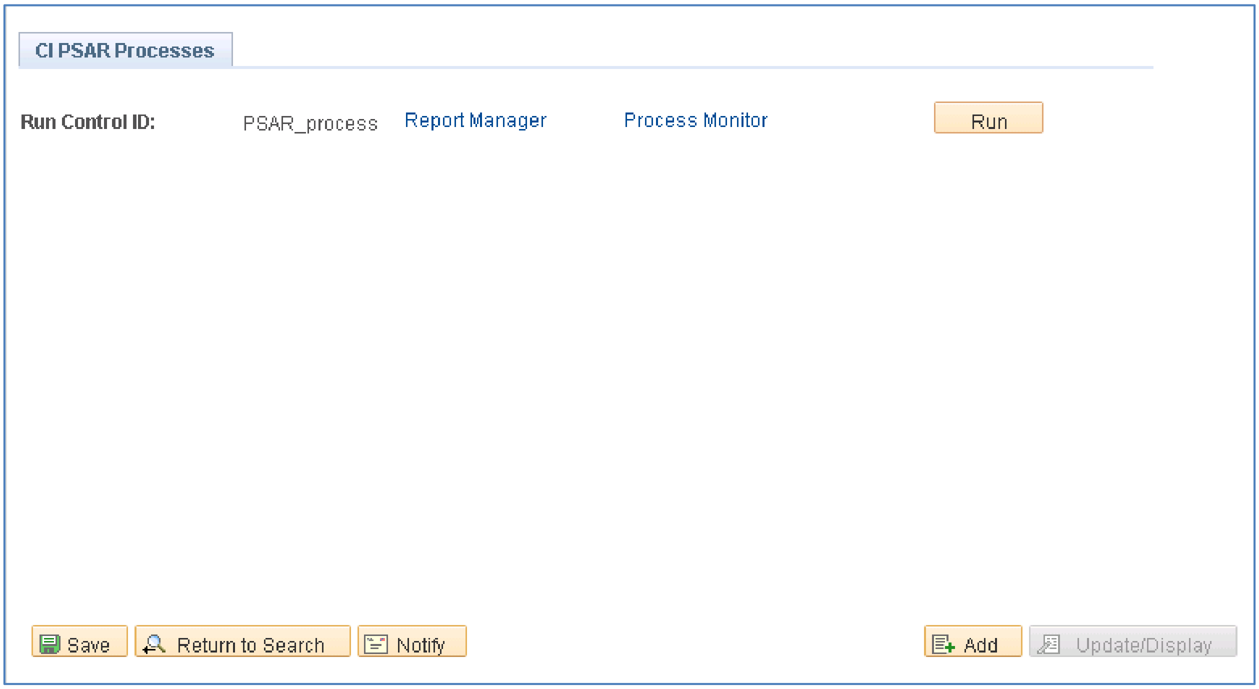
Navigation: CI Customization / Interfaces > CI Security > PSAR Processes > Find an Existing Value (tab)



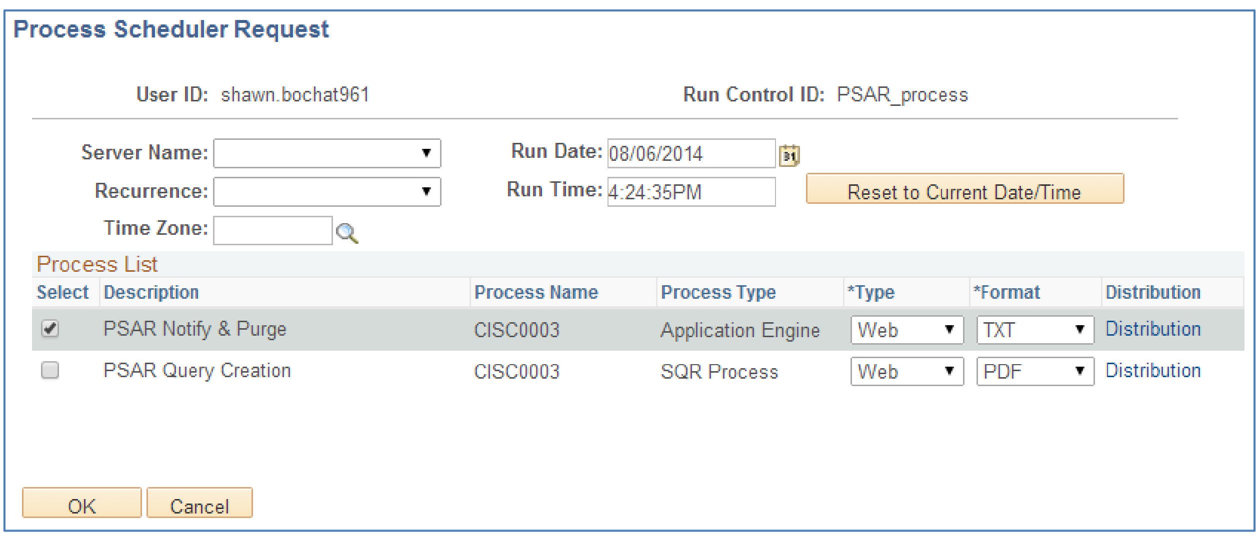
1. **Enter** all or part of a previously setup Run Control ID
2. **Select** the Run Control ID from the Search Results if they appear

6.3 Run the Notification and Purge Process

Navigation: CI Customization / Interfaces > CI Security > PSAR Processes > CI PSAR Processes (tab)



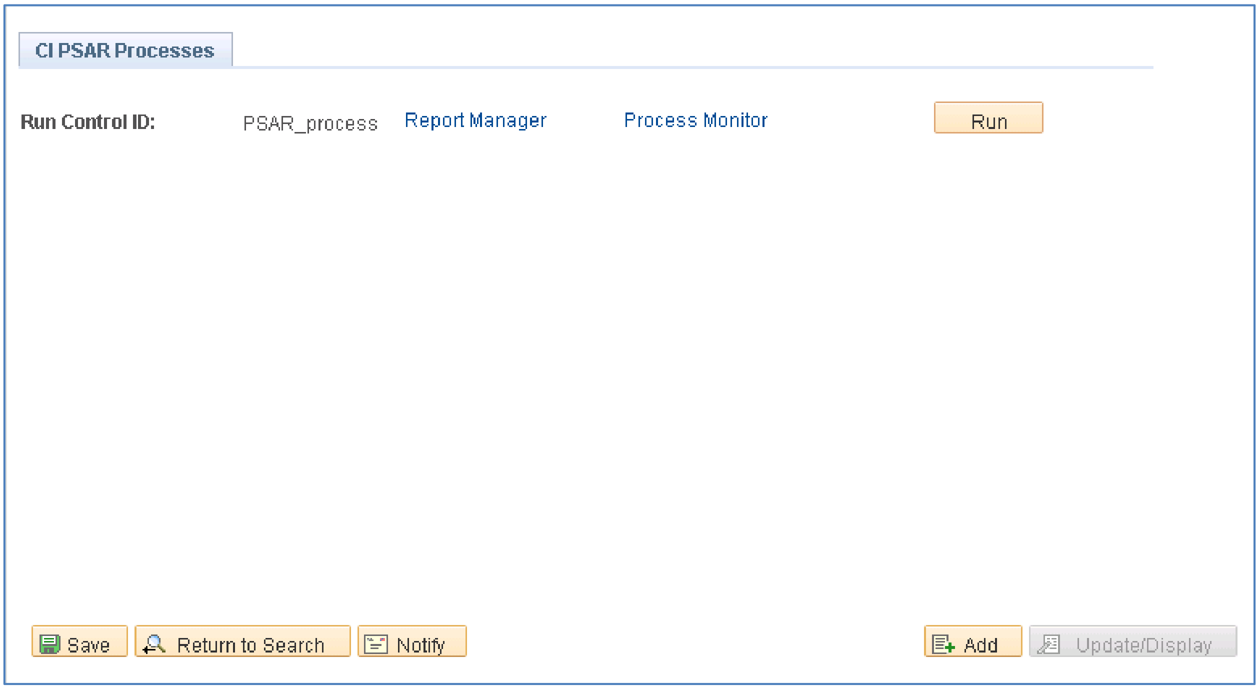
1. After the Run Control is Selected (see Section 6.2), Click **Run** 



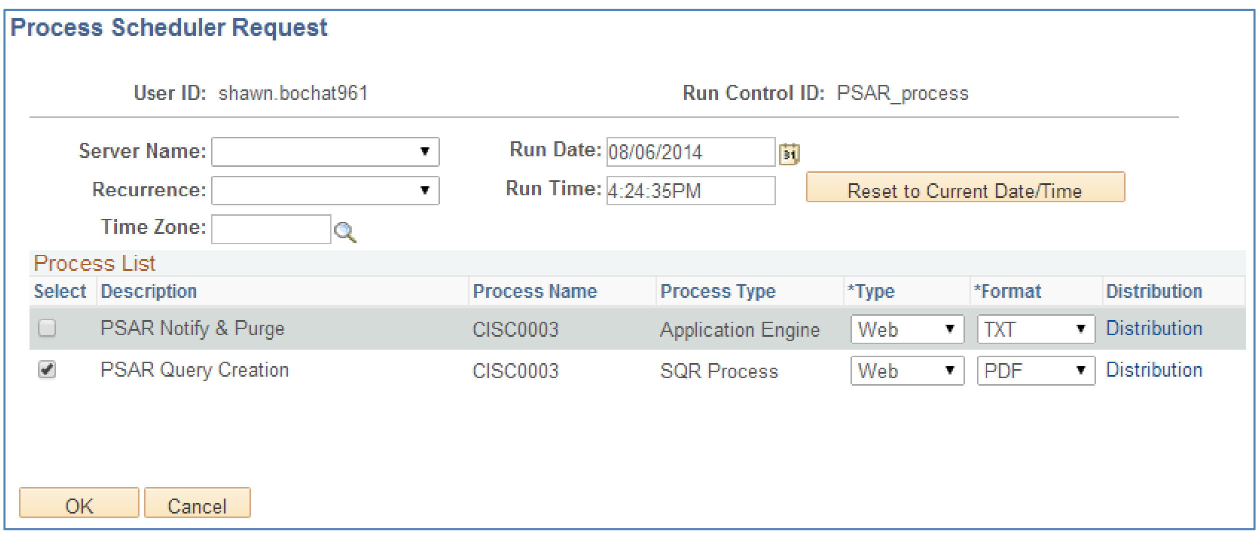
2. **Select** the checkbox next to the PSAR Notify & Purge Description
3. The Type value should be **Web** and the Format value should be **TXT**
4. **Click** OK 

6.4 Run the Create Queries Process

Navigation: CI Customization / Interfaces > CI Security > PSAR Processes > CI PSAR Processes (tab)



1. After the Run Control is Selected (see Section 6.2), Click **Run** 

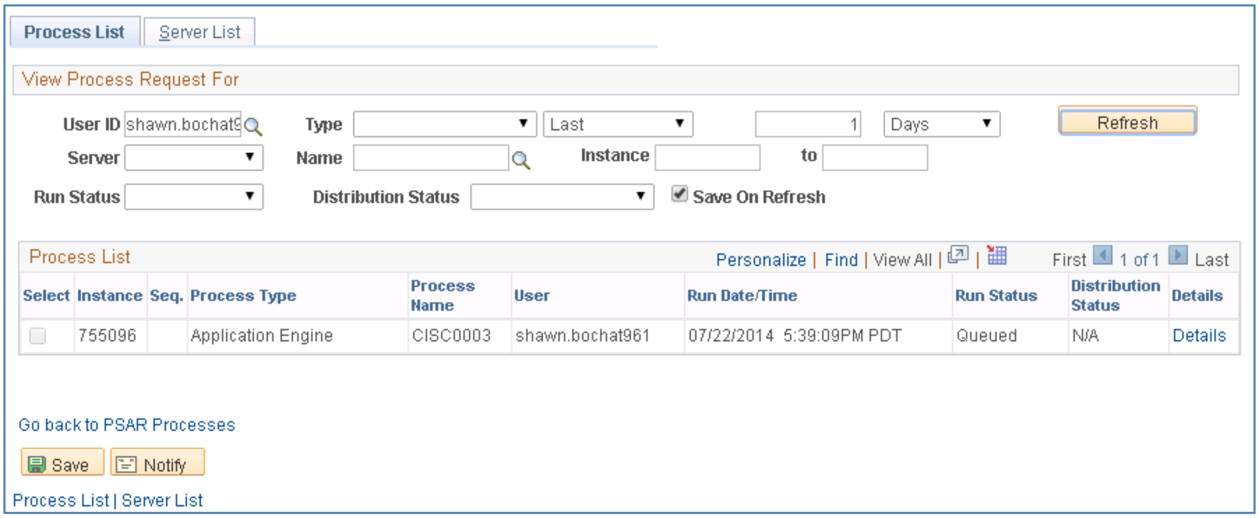


2. **Select** the checkbox next to the PSAR Query Creation
3. The Type value should be **Web** and the Format value should be **PDF**
4. **Click** OK 

6.5 Viewing or Retrieving Process Output

Navigation: CI Customization / Interfaces > CI Security > PSAR Processes > CI PSAR Processes (tab) > Process Monitor (link)

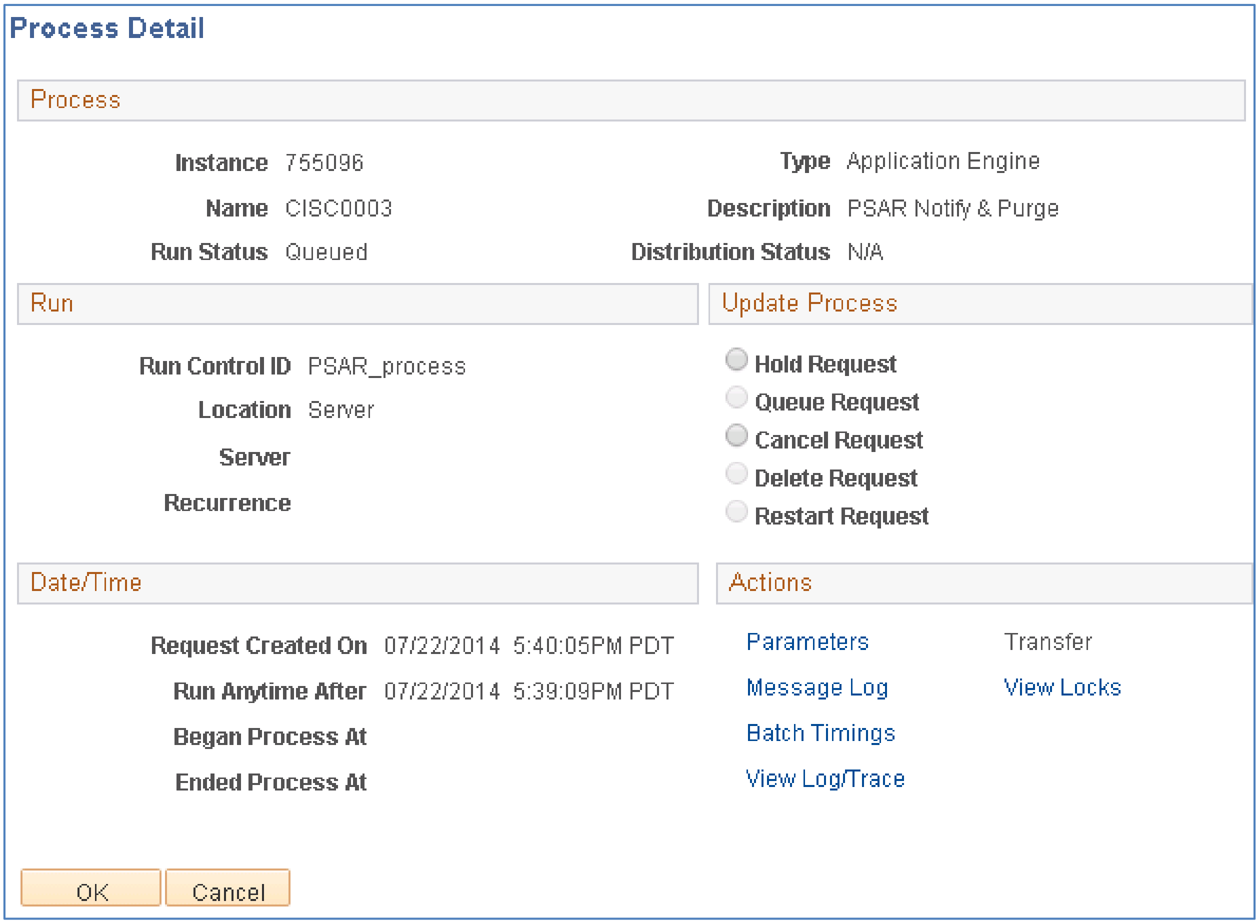
After running either the CISC003 SQR Process (PSAR Query Creation) or the CISC0003 Application Engine Process (PSAR Notify & Purge) from the run control page (Section 6.2 through 6.4) a Process Instance number is displayed on the page.



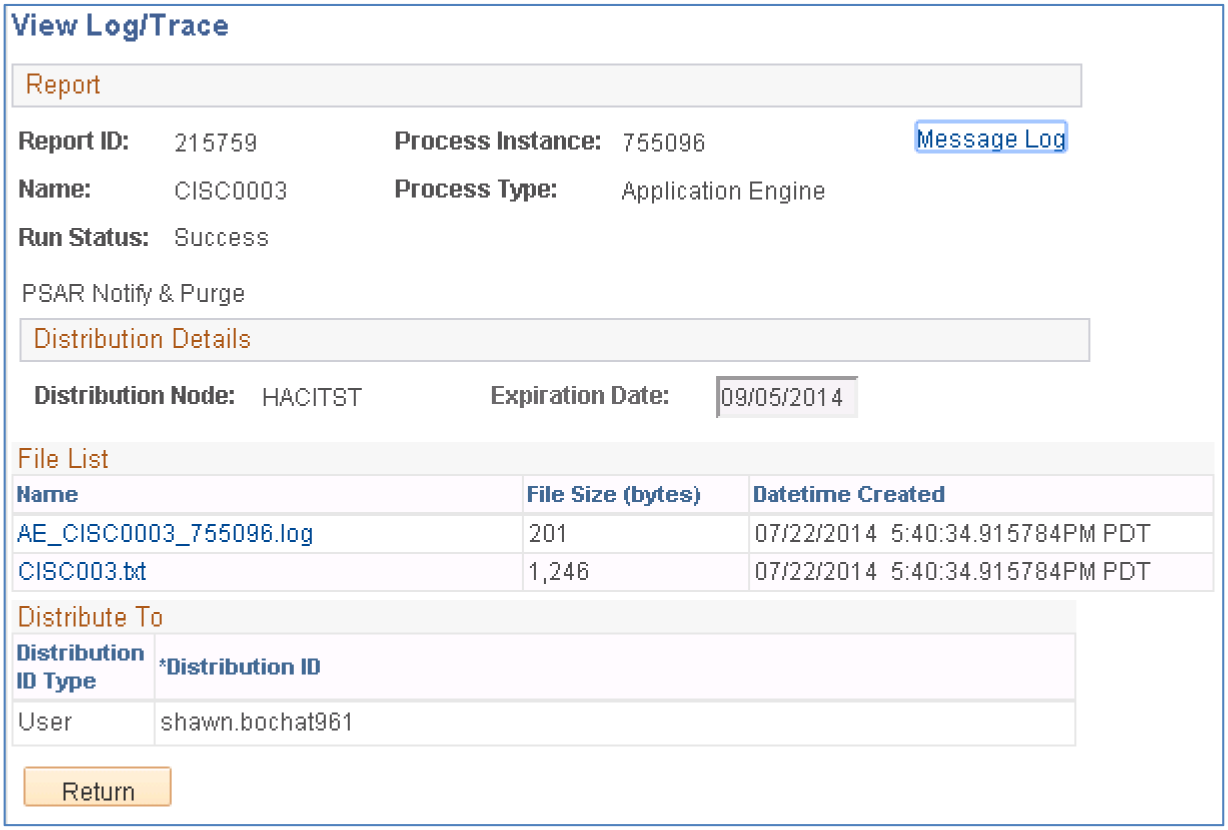
1. **Click** the Process Monitor link after running the Reports To Maintenance Process **OR** navigate to: ***PeopleTools > Process Scheduler > Process Monitor***

2. **Click** the Details link 

in the row that matches your process instance number in the Process List section of the page.



3. **Click** the View Log/Trace link under the Action section for the Process Detail page for the CISC0003 process


View Log/Trace

Report

Report ID: 215759 Process Instance: 755096 Message Log

Name: CISC0003 Process Type: Application Engine

Run Status: Success

PSAR Notify & Purge

Distribution Details

Distribution Node: HACITST Expiration Date: 09/05/2014

File List

Name	File Size (bytes)	Datetime Created
AE_CISC0003_755096.log	201	07/22/2014 5:40:34.915784PM PDT
CISC003.txt	1,246	07/22/2014 5:40:34.915784PM PDT

Distribute To

Distribution ID Type	*Distribution ID
User	shawn.bochat961

Return

4. **Click** the link Under ***Name*** for the file you need in the File List section.

Appendix A – Troubleshooting

This section lists commonly asked questions to resolve access problems.

Appendix B – Documentation Resources

This section lists documentation in addition to this guide that will help with understanding the various aspects of the PeopleSoft System.

CI Functional Documentation

Each area keeps some version of functional documentation. Functional documentation will help explain how data is input and updated as part of the normal business process. No centralized documentation currently exists for all functional documentation at CSUCI. Contact the Module Lead in each area for assistance in understanding the data.

The following process guides have been developed for assistance:

- Design Document
- Process Guide (This Document)

PeopleBooks Documentation

Oracle provides PeopleBooks to help understand the PeopleSoft system. The documentation may seem confusing and abstract at first, but repeated viewing along with reviewing the various business processes will assist in understanding PeopleSoft delivered functionality – such as Query Manager and Query Viewer. The Chancellor's Office maintains the delivered PeopleBooks centrally on the Non-Production login page. This page may only be referenced while on-campus or when a user has accessed the campus network via VPN.

Link: https://cmsdevlauncher.calstate.edu/launcher/indexH.html (Note: Subject to Change)