CHAPTER 1

Securing Campus Community

This chapter discusses how to:

- Set up communication, checklist, and comment (3C) group security.
- Set up service indicator security.
- Replace user security.
- Apply demographic data access security.
- Secure and set up the Population Update process.

Setting Up 3C Group Security

To set up 3C group security, use the 3C Group Security component (OPR_GRP_3C_TABLE).

You can select which 3C groups user IDs can view, update and delete. The Campus Community 3C engine also uses the security that you set up here. Associating a user ID with specific 3C groups allows the user access to specific communication categories, checklist codes, and comment categories. The 3C Deletion process cannot process the user's request to delete 3C items if the Deletion Indicator for the relevant 3C group has not been selected for the user ID.

This section lists a prerequisite and discusses how to grant 3C group security.

Prerequisite

Before you set up 3C group security, set up 3C groups and complete the security setup for your institution.

See Also

lscc, Understanding the 3Cs:Communications, Checklists, and Comments

lsfn, Securing Your Academic Institution

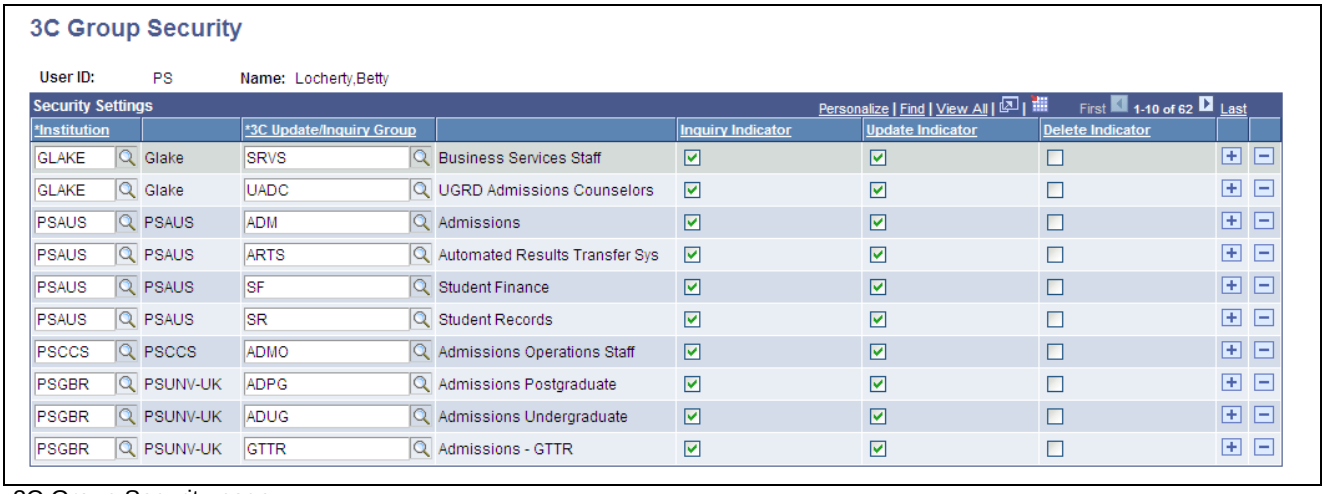
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Page Used to Set Up 3C Group Security

Page Name	Definition Name	Navigation	Usage
3C Group Security	OPR_GRP_3C_TABLE	Set Up SACR, Security, Secure Student Administration, User ID, 3C Group Security, 3C Group Security	Grant user access to 3C group information.

Granting 3C Group Security

Access the 3C Group Security page (Set Up SACR, Security, Secure Student Administration, User ID, 3C Group Security, 3C Group Security).



3C Group Security page

Security Settings

Institution Enter an institution. Only institutions to which this user ID has access are available.

3C Update/Inquiry Group Enter the 3C group that the user ID should have access to for the selected institution. The 3C groups are defined on the Group 3C Table page (GRP_3C_TABLE page).

Inquiry Indicator Select to enable the user ID to *view* all data in the 3C group. The inquiry indicator is used to widen or narrow searches on 3C inquiry pages throughout the system. For example, a user that has inquiry access to a certain 3C group will only be able to view the communications, checklists, or comments assigned to an individual or to an organization that is tied to the 3C group.

Update Indicator Select to enable the user ID to update, by entering or altering, data in the 3C group. You should also select this check box if you want the user ID to be able to process 3C items by using the 3C engine. If the user ID does not have update access to the 3C group, the 3C engine does not process a request by using the 3C group. This functionality is similar to the way the system manages manual assignments for communications, checklists, or comments.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Delete Indicator

Select to enable the user ID to delete data in the 3C group. You should also select this check box if you want the user ID to be able to delete 3C items by using the 3C Deletion process. If the user ID does not have delete access to the 3C group, the 3C Deletion process does not process a request by using the 3C group. This functionality is similar to the way the system manages manual assignments for communications, checklists, or comments.

To be able to delete data, a user must have Update access.

If a user is a member of more than one 3C group and at least one of the groups is enabled for 3C Deletion, then the user is also enabled.

Note. 3C Deletion Policy Manager does not consider 3C group security.

Setting Up Service Indicator Security

To set up service indicator security, use the Service Indicator Security component (SCRTY_TABL_SRVC) and the Service Indicator Display (SCC_SI_DISP_ROLE) component..

This section lists a prerequisite and discusses how to:

- Grant placement and release access to service indicators.
- Restrict display of service indicators.

Prerequisite

Before you set up service indicator security, set up service indicators in the Service Indicator table.

See Also

lscc, Managing Service Indicators

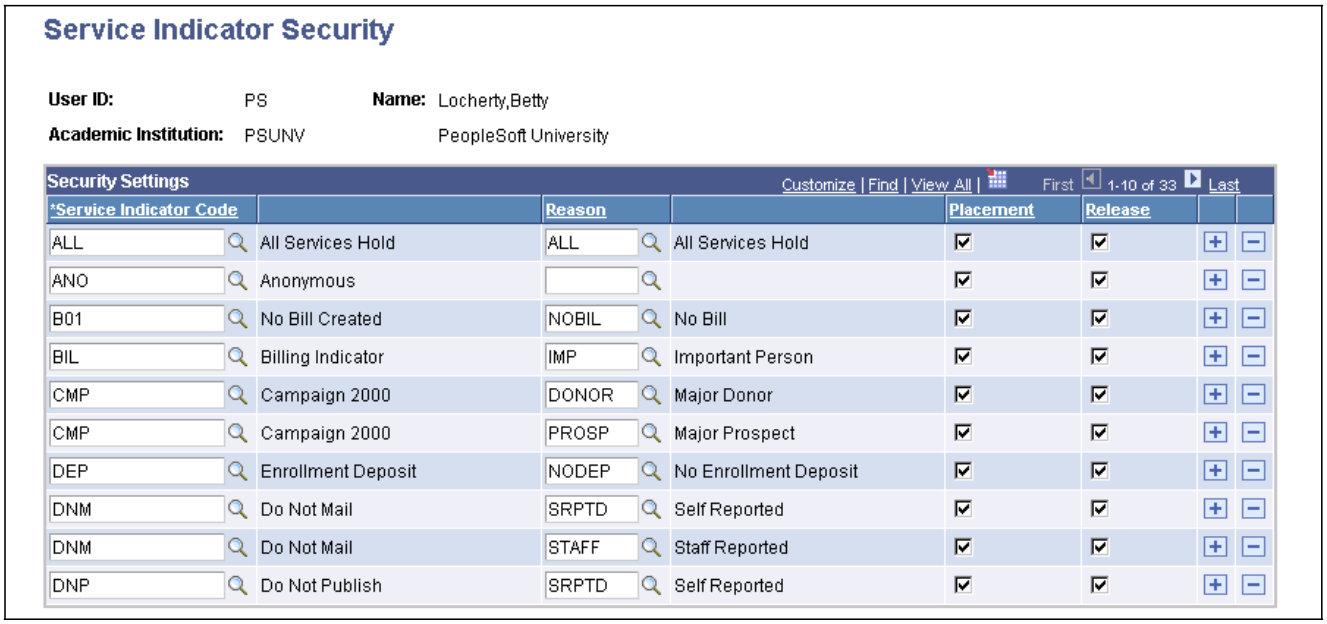
Pages Used to Set Up Service Indicator Security

Page Name	Definition Name	Navigation	Usage
Service Indicator Security	SCRTY_TABL_SRVC	Set Up SACR, Security, Secure Student Administration, User ID, Service Indicator Security, Service Indicator Security	Grant placement and release access to service indicators for a user ID for a particular institution.
Service Indicator Display	SCC_SI_DISP_ROLE	Set Up SACR, Security, Secure Student Administration, Setup, Service Indicator Display, Service Indicator Display	Restrict view access to service indicators on administrative pages to specific roles.

Granting Placement and Release Access to Service Indicators

Access the Service Indicator Security page (Set Up SACR, Security, Secure Student Administration, User ID, Service Indicator Security, Service Indicator Security).

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.



Service Indicator Security page

Security Settings

Service Indicator Code Enter a code for each service indicator that the user ID should be able to place or release. To restrict the use of a service indicator by reason, enter multiple rows for the service indicator and enter the different reasons that apply. You define service indicator codes inside the Service Indicator Table.

Reason Enter a reason indicating when the user ID can access the service indicator. You must enter a reason for each indicator.

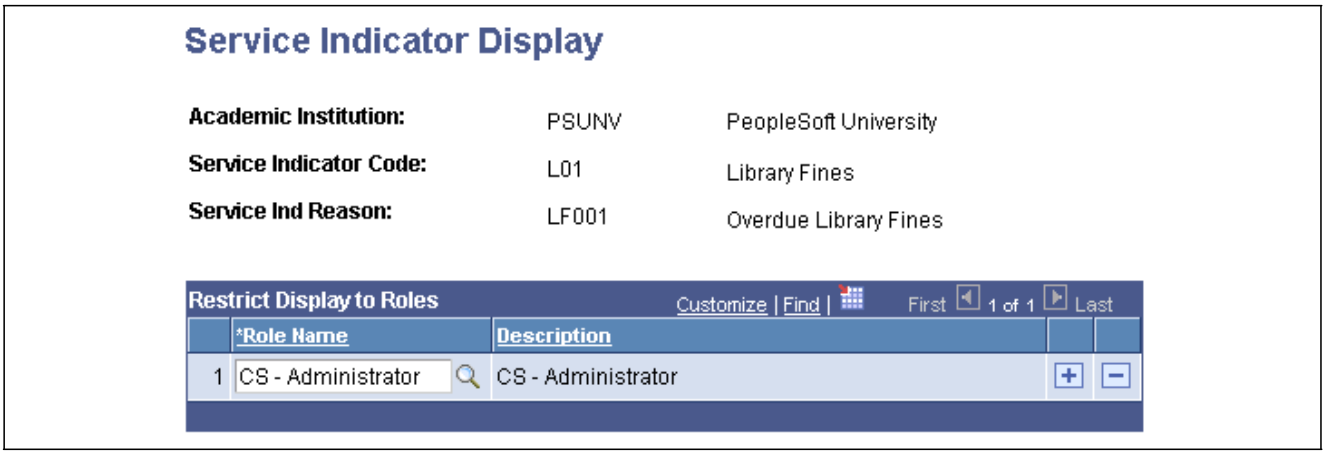
For example, if the user ID should be able to use the conference guest service indicator only for football recruitment visits or Special Olympics guests, select each of those reasons for the conference guest service indicator. Define the reasons for using a service inside the Service Indicator table.

Placement and **Release** Select if this user ID should have permission to assign or release the service indicator.

Restricting Display of Service Indicators

Access the Service Indicator Display page (Set Up SACR, Security, Secure Student Administration, Setup, Service Indicator Display, Service Indicator Display).

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.



Service Indicator Display page

Restrict Display to Roles

To restrict the display of a service indicator's data to specific roles, enter the one or more roles for whom the data should appear. The system displays the data only for the roles that you specify, and does not display it for any role not listed.

If you do not want to restrict the display, ensure that no role is listed. When no role is listed on the Service Indicator Display page, the service indicator data is unrestricted and the system displays it for all roles.

Service indicator data includes the service indicator icon on pages for IDs to which the indicator is assigned, and the service indicator information on the Service Indicator Summary page and the General Info tab of the Student Services Center component.

Note. A user's placement or release security takes precedence over restricted display. If the display of a service indicator is restricted, but the user has place or release access for that service indicator, then the service indicator data will appear for that user whether or not the user has any of the restricted display roles.

Replacing User Security

To copy or assign Campus Solutions user security, use the User Security Replacement component (SCRTY_OPRID_REPLAC) or the Mass User Security Replacement component (SCC_MASS_SCRTY_UPD).

Copying a security setup is the same as going to each appropriate menu and entering data for each security object to assign security for a specific user. Replacement security automates the process for you by enabling you to copy a security profile either to another individual user or to several users in mass.

This section discusses how to:

- Replace user security for an individual.
- Replace user security for multiple individuals.

Note. User security replacement described here applies only to Campus Solutions user security. It does not apply to PeopleTools security.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Pages Used to Replace User Security

Page Name	Definition Name	Navigation	Usage
User Security Replacement	SCRTY_OPRID_REPLAC	Set Up SACR, Security, Secure Student Administration, Setup, User Security Replacement, User Security Replacement	Copy the security setup of one user to another user.
Mass User Security Replacement	SCC_MASS_SCRTY_UPD	Set Up SACR, Security, Secure Student Administration, Process, Mass User Security Replacement, Mass User Security Replacement	Assign or copy a security profile to an individual user or to a group of users.

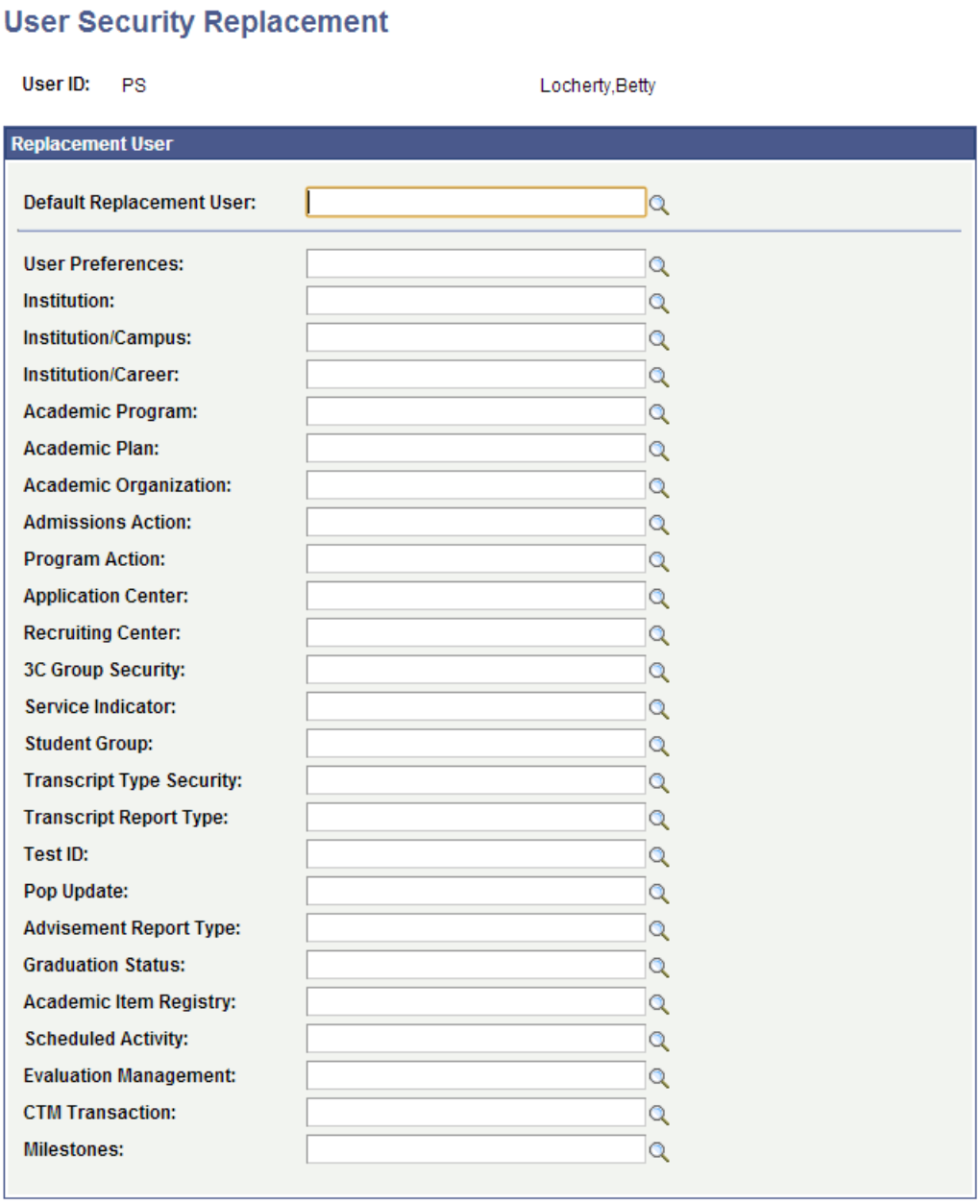
Replacing User Security for an Individual

Bundle 32

****This screenshot is updated****

Access the User Security Replacement page (Set Up SACR, Security, Secure Student Administration, Setup, User Security Replacement, User Security Replacement).

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.



User Security Replacement page

Replacement User

Default Replacement User

To replace or create all of a user ID's security objects with the same security objects assigned to another user ID, specify the user ID whose security objects you want to copy in this field. When you exit the field, the system automatically copies each security object from the replacement user ID.

If you do not want to replace each of this user's security objects with all the security objects of one user ID, indicate the replacement user ID for each object that you want to replace. You do not have to replace all objects. For those objects that you do not want to replace, leave the field blank.

User Preferences

When you enter a user ID in this field, the default values that you set up in the User Default component for the entered user ID are assigned to the user

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

ID, including the enrollment override defaults which assigns the Enrollment Access ID.

User defaults are set up in the User Defaults component.

See lsfn, Setting User Defaults.

3C Group Security When you enter a user ID in this field, the system also sets the values on the User 3C Group Summary page of the User Defaults component.

When you enter a user ID in any of the other fields on this page, the user ID is assigned the same security that you set up for the selected user ID for that item. All of these fields refer to the security that you set up on the pages in Set Up SACR, Security, Secure Student Administration, User ID.

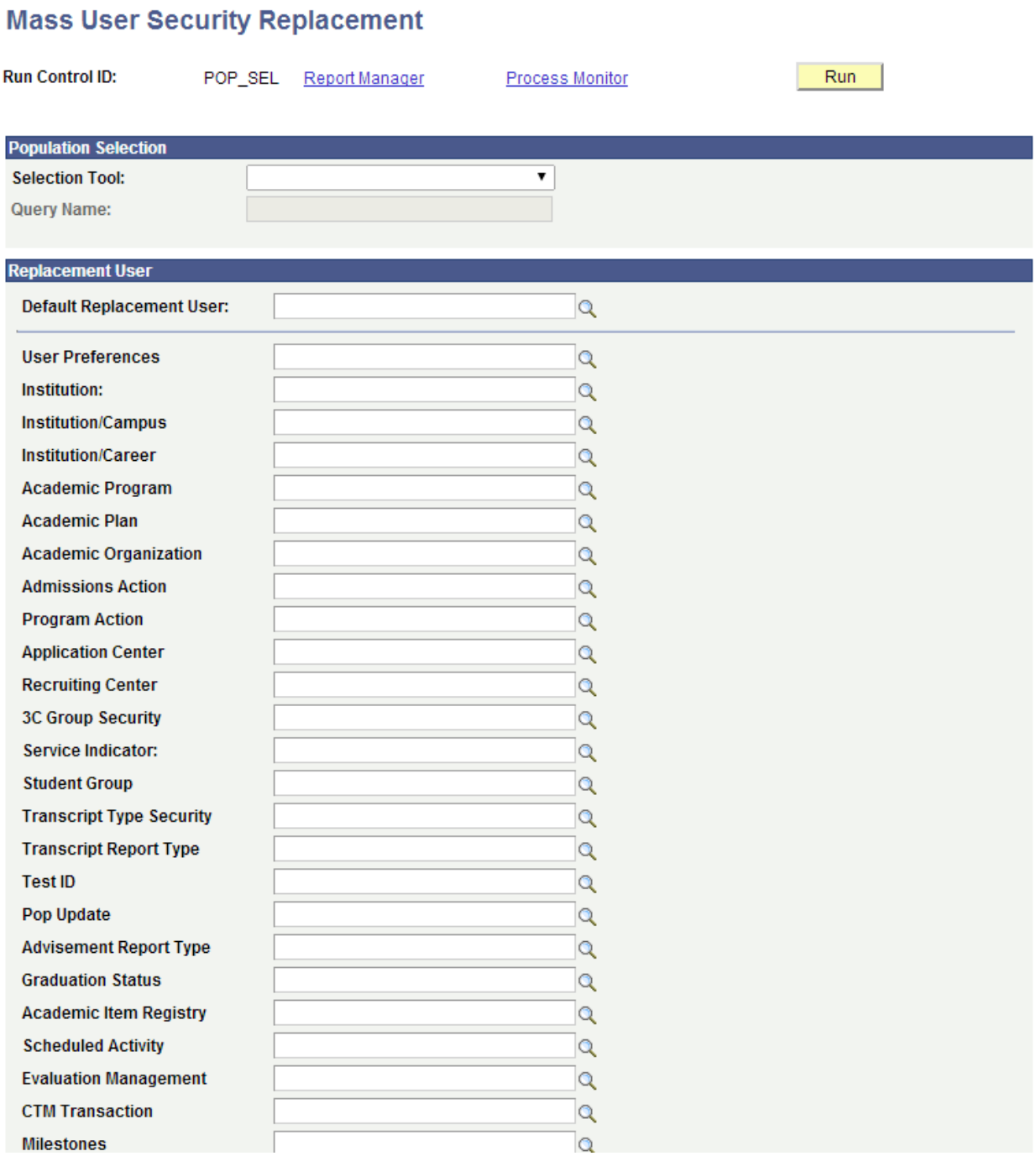
Replacing User Security for Multiple Individuals

Bundle 32

****This screenshot is updated****

Access the Mass User Security Replacement page (Set Up SACR, Security, Secure Student Administration, Process, Mass User Security Replacement, Mass User Security Replacement).

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.



Mass User Security Replacement page

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Population Selection

Enter the tool and related parameters for selecting the population of user IDs to which you want to assign this user security or replace the existing security.

Fields in the Population Selection group box on this page function the same as they do in the Population Selection group box across the system.

See lscc, Using the Population Selection Process.

Replacement User

Enter the user ID whose security you want to mass assign to the user IDs selected by Population Selection. You can modify any of the user security values to assign.

Fields in the Replacement User group box function the same as described for the same group box on the User Security Replacement page.

Applying Demographic Data Access Security

To set up demographic data access (DDA) security, use the Demographic Data Access component (PERS_MSK_CFG) and the Demographic Data Access process component (RUNCTL_MSK_CFG).

This section provides overviews of DDA security and setting up DDA security, and discusses how to:

- Define DDA masking configurations.
- Run the DDA process.

Understanding DDA Security

With DDA security, you can mask the display of national ID and birth date data in search records, prompt records, and on the Bio/Demo Data and the Relationships pages if these pages have display-only security. You can mask entire fields, the first five characters of the national ID field, or the year of the birth date field. You can apply masking to one, both, or neither field. No matter which masking configuration you use, users can search on the entire national ID field.

Note. To enhance the flexibility of masking for the National ID and birth date in Search/Match functionality, see Search/Match display options. National ID and birth date data are not masked in queries and reports.

See lscc, Setting Up Search, Match.

To apply DDA security, you define masking configurations for all primary permission lists and assign a primary permission list to each user ID as part of his or her User Profile.

For example, suppose a primary permission list assigned to a user ID is named ALLPANLS. You might not want national IDs to appear throughout the system for this permission list, but you do want partial birth dates to appear. You would access the Demographic Data Access setup page and insert a row for the ALLPANLS permission list. In that row, you would configure the system to both mask the entire national ID and display a partial birth date field (masking the year).

You must then run the Demographic Data Access (MSK_CFG) process to replace data in the masking configuration table with the masking configuration that you defined. The new configuration will be applied to each user to whom that permission list is assigned.

 Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

In the example, after running the Demographic Data Access process, each user whose primary permission list is ALLPANLS will not see national IDs on search pages or prompts, but they will see the birth month and day where birth dates appear. The masking configuration for the primary permission list to which a user is assigned also controls how national ID and birth date data appear on the Bio/Demo Data page (SCC_BIO_DEMO_PERS) and the Relationships page (RELATIONSHIPS) throughout the system.

Note. The national ID and the birth date fields appear masked on the Biographical Details page and the Relationships page only for users who have security set to show the pages in display-only mode. If a user has more than one permission list and, therefore, has both add/update and display-only access to a masked page, then the least restrictive setting (add/update) takes precedence, and masking is not applied.

Setting Up DDA Security

To set up DDA security, you must assign a primary permission list to each user ID, grant administrative access to components for managing DDA, and define masking configurations for each primary permission list.

Note. All Campus Solutions search records and prompts depend on DDA security. Therefore, you must assign a primary permission list to each user, even those who do not need the national ID and the birth date fields masked. In the latter case, set the masking configurations in the primary permission list for both the National ID and the Date of Birth to *Display entire field.*

Pages Used to Apply DDA Security

Page Name	Definition Name	Navigation	Usage
General	USER_GENERAL	PeopleTools, Security, User Profiles, User Profiles, General	Assign a primary permission list to a user ID.
Pages	ACL_MENU2	PeopleTools, Security, Permissions & Roles, Permission Lists, Pages	Grant access to new components for managing DDA masking configurations for each primary permission list. Grant access to new Student components for users that should prompt only against Students.
Demographic Data Access (setup)	PERS_MSK_CFG	Set Up SACR, Security, Secure Student Administration, Permission List, Demographic Data Access, Demographic Data Access	Define masking configurations for primary permission lists.
Demographic Data Access (run control)	RUNCNTL_MSK_CFG	Set Up SACR, Security, Secure Student Administration, Process, Demographic Data Access, Demographic Data Access	Initialize the primary permission list configuration for all primary permission lists assigned to users.

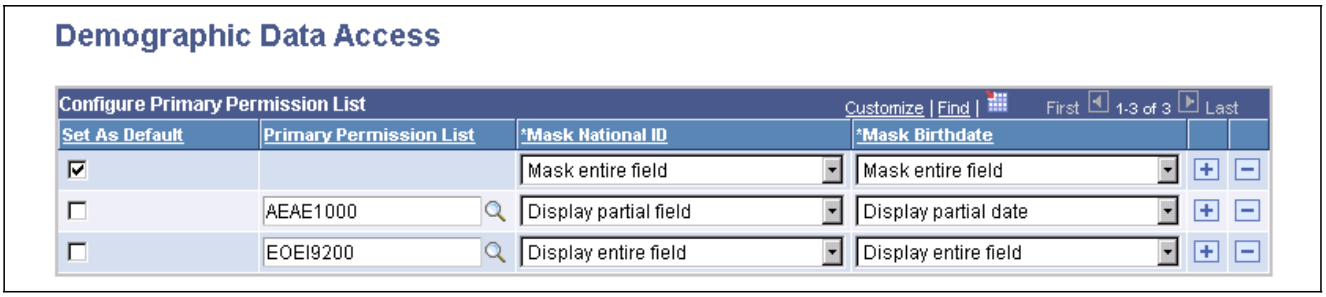
See Also

PeopleTools PeopleBook: Security Administration, "Setting Up User Profiles" and "Working with Permission Lists"

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Defining DDA Masking Configurations

Access the Demographic Data Access (setup) page (Set Up SACR, Security, Secure Student Administration, Permission List, Demographic Data Access, Demographic Data Access).



Demographic Data Access (setup) page

Important! Each time you make changes to the Demographic Data Access page, you must run the DDA process to apply the changes.

Configure Primary Permission List

Set As Default

Select to assign this masking configuration to all permission lists used as primary permission lists.

When selected, the Primary Permission List field becomes unavailable.

Primary Permission List

Insert a row for each primary permission list that requires a masking configuration different than the default masking configuration.

When you run the process, the system applies this masking configuration to all users to whom this primary permission list is assigned.

Mask National ID

Enter the configuration to use for national IDs. Values are *Display entire field*, *Display partial field*, and *Mask entire field*.

If you display a partial field, the system masks the first five characters of the national ID field.

These translate values should not be modified.

Mask Birthdate

Enter the configuration to use for birth dates. Values are *Display entire field*, *Display partial date*, and *Mask entire field*.

If you display a partial date, the system masks the year and displays month and day in the default date format for each birth date field.

These translate values should not be modified.

Running the DDA Process

Access the Demographic Data Access (run control) page (Set Up SACR, Security, Secure Student Administration, Process, Demographic Data Access, Demographic Data Access).

Copyright © 2012, Oracle and/or its affiliates. All rights reserved.

Demographic Data Access (run control) page

You must run the DDA process (MSK_CFG) to apply changes made on the Demographic Data Access (setup) page and to apply the default masking configuration to any newly created, newly assigned primary permission list whose masking configuration is not otherwise defined.

Note. The process applies the masking configuration only for permission lists that are used as "primary" permission lists. Therefore, if you assign a User ID a primary permission list that was not used as the primary the last time the DDA process was run, you will need to run the process again.

Securing and Setting Up the Population Update Process

To secure and set up the Population Update process, use the Population Update Security (SCC_POP_UPD_SRTY) component and the Population Update Setup (SCC_POP_UPD_SETUP) component

This section discusses how to:

- Assign Population Update user security.
- Set up the Population Update process.

See Also

lscc, Using the Population Selection Process, Running the Population Update Process, Understanding the Population Update Process

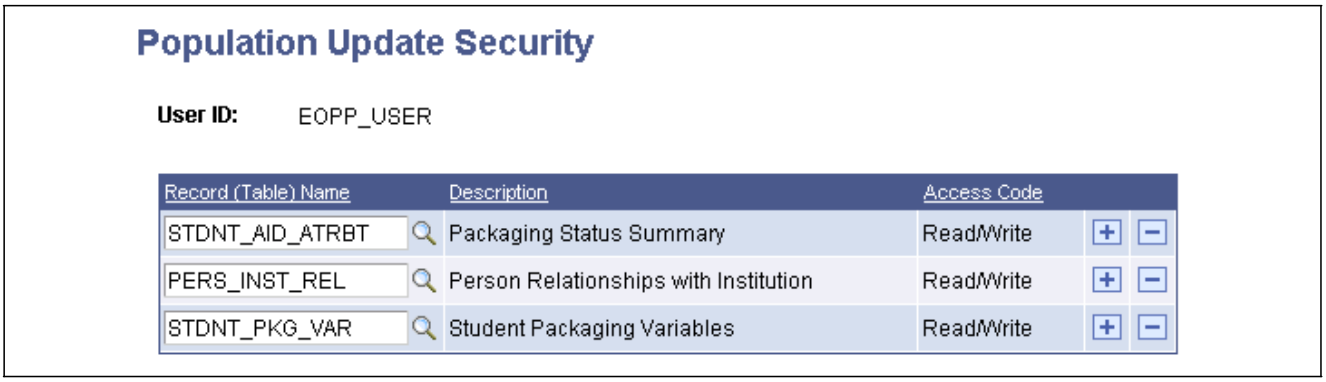
Pages Used to Secure and Set Up the Population Update Process

Page Name	Definition Name	Navigation	Usage
Population Update Security	SCC_POP_UPD_SRTY	Set Up SACR, Security, Secure Student Administration, User ID, Population Update Security, Population Update Security	Set user security for accessing records to update using the Population Selection update process.
Population Update Setup	SCC_POP_UPD_SETUP	Set Up SACR, System Administration, Utilities, Population Update, Population Update Setup, Population Update Setup	Identify records and fields to make available for updating.

Assigning Population Update User Security

Access the Population Update Security page (Set Up SACR, Security, Secure Student Administration, User ID, Population Update Security, Population Update Security).

Copyright © 2012, Oracle and/or its affiliates. All rights reserved.



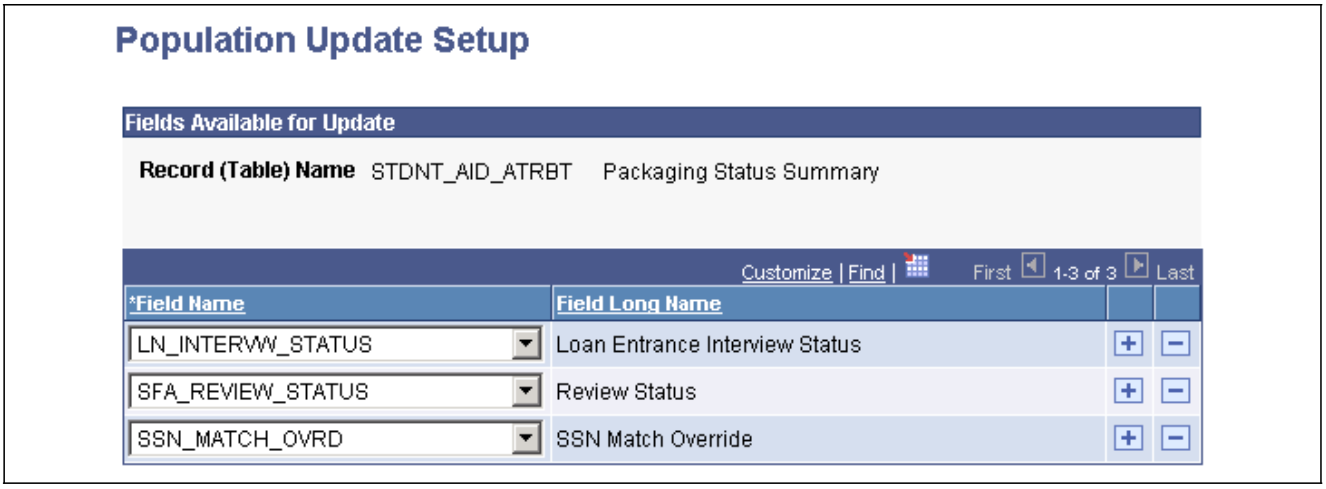
Population Update Security page

Record (Table) Name Enter each record that you want the user to be able to update for populations selected by the Population Selection process.

After you save the page, the user can view and update the records if your institution or department makes them available for updating on the Population Update Setup page.

Setting Up the Population Update Process

Access the Population Update Setup page (Set Up SACR, System Administration, Utilities, Population Update, Population Update Setup, Population Update Setup).



Population Update Setup page

When you select a record and access the Population Update Setup page, the system makes the fields from that record available in the Field Name drop-down lists. Select each field that you want to make available for users to update. Only the records and fields that you select and to which the user has security access will be available on the run control page.

Copyright © 2012, Oracle and/or its affiliates. All rights reserved.