Setting Up and Using New User Registration Framework

Understanding New User Registration

New User Registration is a framework that enables a user to sign in to the Campus Solutions system in order to complete a specific online self-service transaction. For example, on your institution's portal you could indicate the steps a future applicant should perform in order to apply online. In this case the specific online self-service transaction is the online application. You can provide a link to transfer the user to your Campus Solutions database where the future applicant first needs to sign in. Going through New User Registration, the user can either create a user ID and password, or use an existing user ID to sign in to your system. New User Registration assigns the newly created user profile with generic security roles that are required to access your system. When the user profile is created or when the user uses an existing user ID, New User Registration assigns security roles to the user profile that are specific to the online transaction to which the New User Registration framework is integrated. Once the user is authenticated, New User Registration immediately redirects the user to a predefined target page that is related to that specific online transaction.

In a nutshell, New User Registration offers user validation, user registration, system authentication, generic and specific (just-in-time) security provisioning, and easy navigation access by transferring the newly authenticated user to a predefined target page specific to the online self-service transaction the user elected to perform.

Consider this example. If you use Admission Applications Web Services (AAWS) and deployed an online application self-service component, an online applicant first uses New User Registration to register for a user ID (or first get authenticated if the applicant already has a user ID) and then perform the online application transaction, such as submitting an application. In this case, after being successfully authenticated to your system, the system provisions the applicant's user profile with the role security specific to access your online application page and then immediately redirects the applicant to this online application page. Another example is, if you are using the Delegated Access feature, a person who received delegated access (a proxy) could first use New User Registration to access your system by either creating a user ID or reusing an existing user ID. Once successfully authenticated through New User Registration, the system could provision the proxy's user profile with a security role needed to access the Delegated Access initial page (the Proxy Terms and Conditions page).

New User Registration provides web service operations that you can use on your user interface to:

- Create a user account (user ID) (SCC_USERREG_CREATEACCT)
- Authenticate a user (SCC_USERREG_AUTHENTICATE)
- Retrieve a user ID (SCC_USERREG_GET_USERID)
- Reset a password (SCC_USERREG_GET_PASSWORD and SCC_USERREG_GET_PSWD_HINT)

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

- Check if authenticated users have the proper security role (authorization) (SCC_CHECK_AUTH)

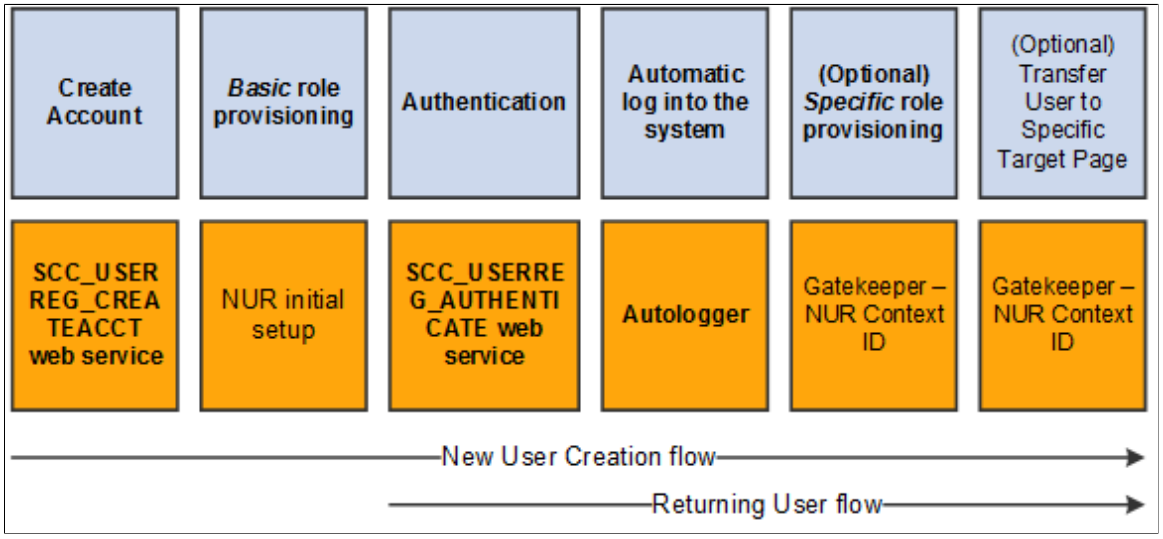
Also, New User Registration is a consumer of the Constituent Transaction Management (CTM) framework (delivered CTM transaction code is NEW_USER_REGISTRATION). This allows staging of any constituent information that is entered at the time of registering a new user ID. For example, when creating a user ID you may want to ask users to enter their name, email address, and so on. If the online transaction integrated with New User Registration is defined as a CTM transaction, it can reuse or display the constituent data that was entered at registration time in the self-service transaction pages (that is, if the CTM transaction is partitioned by constituent).

Your system is provided with two sample login pages: New User Registration login sample page and New User Registration Tester page. Both are visually similar and allow a user to create a user ID or use an existing user ID to access your system. The New User Registration login sample page is fully integrated with all the New User Registration framework security objects. It is an example of how your own custom login page can be integrated and deployed with New User Registration. For example, it can reside outside of your firewall and be set as a Kiosk. The New User Registration Tester page can be used by your developers to test and evaluate the New User Registration framework objects. The Tester page contains the same functionality included in the New User Registration login sample page, but is meant to be used inside the same database. This page should be used *only* for testing purposes and should *not* be deployed in a production environment.

The following diagram shows the workflow for a new user and a returning user when New User Registration framework is deployed:

Image: New User Registration User Flows

New User Registration User Flows



The first row of boxes indicates the steps in the workflow for a new or returning user. The second row indicates what needs to be set up so that the user can perform the step.

Related Links

Using the New User Registration Sample User Interfaces
New User Registration Web Service Operations
Developer Reference to Deploy New User Registration
Understanding CTM

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

New User Registration Terminology

The following terms are important to the understanding of New User Registration framework and are used throughout the documentation.

Term	*Description*
Guest	New user. A person who is unknown to the Campus Solutions system and who wants to perform an online transaction. A guest needs to register for a user ID to access the system.
Returning User	A person known to the Campus Solutions system and who wants to perform an online transaction. This person uses an existing user ID and password to access the system.
CTM	Constituent Transaction Management. This is a framework that allows a user to perform an online transaction without having an EMPLID known. CTM stores the constituent and the transaction-specific data in staging records. The system assigns an EMPLID only after the user saves or submits the online transaction. Using CTM allows no interruption for a user to complete an online transaction because the process that the system uses to assign an EMPLID is completely transparent to the online user.
Online transaction or online self-service transaction	This refers to the transaction that consumes the New User Registration framework.
Login page	The page used to access the Campus Solutions system. The login page is integrated with the New User Registration framework security objects. Institutions customize the sample login page or use their own page to comply with their security management requirements.
Target page	The page to which the guest or the returning user is redirected after being authenticated through the New User Registration framework. The target page is defined in the New User Registration Context setup component.
Landing page	The page to which the guest or user is redirected before registration and authentication by the system.
Autologger	An object that the New User Registration framework delivers. This object allows signing in the guest or the returning user directly into your system after being successfully authenticated.
Gatekeeper	A utility that the New User Registration framework delivers. This utility acts as a router for all requests from external clients wishing to access Campus Solutions self-service pages. An external client is a user interface that is built by an institution and that lie outside the PeopleSoft system. The Gatekeeper uses the New User Registration Context ID to provision application-specific security role and transfer the user to a specific target page after authentication.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Term	*Description*
SwitchUser	A PeopleTools function used by the New User Registration Tester sample page to autolog the guest's or the returning user's entered user ID. The function switches a signed in user to another one.
Anonymous user	When the guest elects to create a new user ID, he or she is first considered an anonymous user by the system.
Provisioning	New User Registration provisions security roles at two levels: Basic provisioning: When a guest creates a new user ID though New User Registration, basic roles are provisioned to the newly created user profile. Basic roles grant access to generic information that all users are required to have to access and navigate in your system. This provisioning is required. Specific provisioning: When a New User Registration Context is used, the guest or the returning user is provisioned just-in-time after being authenticated with application level security. The security provisioning done here is specific to the application integrated with New User Registration. This provisioning is optional.

Constituent Transaction Management and New User Registration

You can configure your login page to request additional personal information such as first name, last name, email address and so on when a user creates a new user ID. To store this information in the production tables, an EMPLID is required. If the user does not have an EMPLID at the time of registration, New User Registration uses the Constituent Transaction Management (CTM) framework to store the personal information in the CTM constituent staging tables. During this process, the system enters the information using a temporary ID (SCC_TEMP_ID), and uses the CTM transaction code NEW_USER_REGISTRATION that is delivered with your system. If New User Registration is followed by a subsequent CTM online transaction (and that CTM transaction is set up to be partitioned by constituent), the system can gather additional personal information, create or assign an EMPLID, then promote the staged constituent data to the respective production tables.

 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The following diagrams show where CTM takes place as part of the New User Registration flow:

Image: Create Account Page for New Users

This example illustrates the fields and controls on the Create Account Page for New Users. You can find definitions for the fields and controls later on this page.

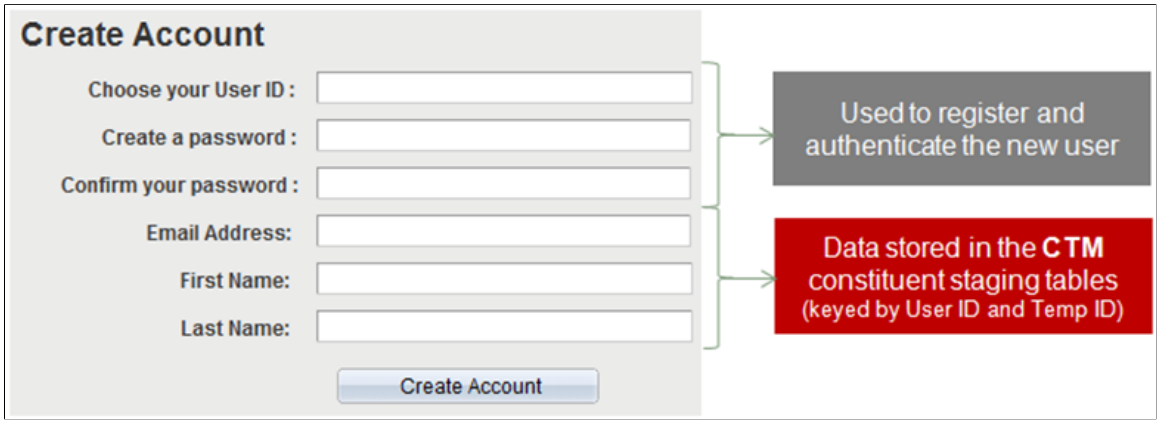


Image: Login Page for Existing Users

This example illustrates the fields and controls on the Login Page for Existing Users. You can find definitions for the fields and controls later on this page.

When New User Registration consumes CTM, the system does not trigger the process to create EMPLIDs. This prevents non-serious individuals from creating user records for themselves in your system and populating your database with dummy names or with users that never pursue any other actions with your institution. To prevent this, CTM triggers Search/Match only when the guest performs a subsequent transaction such as an online application. Only then is the constituent data considered valid.

Note: CTM is not involved when an existing user signs into your system through New User Registration. This is because at the time of authentication the returning user is typically only asked to enter a user ID and a password.
The self-service online transaction that you integrate with New User Registration does not need to be a CTM transaction. A self-service online transaction is usually configured for CTM when the data provided by the self-service user needs to be staged before it is moved to the production tables, or when an EMPLID needs to be associated with the self-service user. Using CTM allows for no user interruption to assign an EMPLID. If the integrated self-service online transaction does not require an EMPLID to be assigned or no data to be staged, it can still be integrated with New User Registration.
See Setting Up CTM for New User Registration.

Notifications Framework and New User Registration

The New User Registration framework uses the Notifications framework as part of the Forgot User ID utility. New User Registration triggers the Notifications framework from the New User Registration sample login page or New User Registration Tester page. When users click the Forgot your User ID link and enters their address, the system validates the email address and the user ID is retrieved. The Notifications framework sends an email to the user that contains the user's ID.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

An email template for sending an email message that contains the user's ID is delivered with your system. It uses a custom logic to retrieve the user's email address. This logic is delivered with your system and it matches the email address in the user's profile with the email address users provide when they use the Forgot User ID utility. The custom logic is contained in the application class SCC_IDENTITY_MGR:NOTIFICATION:NURCustomLogicprovider.

Notification Templates for New User Registration

Email templates are delivered with your system. These generic templates establish a common format for notifications.

Template Name	*Description*	*Trigger*	*Recipient*
NUR_EMAIL_OPRID	A basic email that includes the user ID of the requestor. Example: Email Subject: Your User ID to access the Campus Solutions system. Email Message: You are receiving this email message because you had forgotten your User ID to access the Campus Solutions system.Your User ID is TEST100 This is an auto generated email; please do not respond to this message.	When a user clicks the Forgot your User ID link on the New User Registration sample login or Tester page. The user provides an email address, which the system validates. When the email address is valid, the user ID is retrieved and is sent through an email message.	Users who have forgotten their user IDs.

To modify the template, go to PeopleTools, Workflow, Notifications, Generic Templates.

Currently, only the following variables are defined and delivered with the Forgot User ID utility. Adding more variables requires substantial programming effort.

- %1 => OPRID
- %2 => URL Link (not used in the delivered template)

Warning! Notifications are intended to be short and simple messages with the purpose of informing about a specific subject. The list of variables contained in each message is delivered with your system and require extensive coding effort to be modified.

Note: As part of New User Registration framework, only the Forgot User ID utility consumes the Notifications framework. The Forgot Password utility uses the PeopleTools Send Password Email utility.

See Understanding the Notifications Framework

New User Registration Context

A New User Registration context is optionally used when the New User Registration framework is consumed by a specific self-service online transaction. A New User Registration context is defined

 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

through a New User Registration context ID. The context ID is an *optional* element. You embed the context ID in a URL that is used to transfer a user to the New User Registration login page. You need a New User Registration context ID if you want to seamlessly assign application-specific security roles to the newly authenticated user, and then transfer the user to the target page for the self-service online transaction that the user wants to access. The Gatekeeper uses the Context ID that you include in the URL to grant the user the required security roles, and to access the target page.

The New User Registration Context ID is read by the Gatekeeper immediately after a user is successfully authenticated into your system. The New User Registration Context ID defines the security roles that the system should assign to the user. This ensures that the user has the required security roles to be automatically transferred to the target page for that specific self-service transaction and perform the online transaction. Both security provisioning and page transfer occur after a guest or returning user is successfully authenticated by New User Registration into your system. You can define a New User Registration Context for each online self-service transaction that you integrate with New User Registration. Each transaction has its own security provisioned and target page information.

To define a New User Registration Context, use the New User Registration Context page (SCC_APPL_CONTEXT). The security provisioning is defined by roles and the target page can either be a PeopleSoft Internet Architecture (PIA) page defined in your PeopleSoft system or a URL to an external site. Provisioning security or transferring to a target page is optional. Create a New User Registration Context for your integrated self-service transaction only if you want to provision specific security for the transaction or to transfer the user directly to a target page related to the self-service transaction.

You can create a default New User Registration Context ID. If there is no New User Registration Context ID in the URL when a user accesses the New User Registration login page, the default context ID is used to provision security or transfer the user to a target page. In this case, you should set up your default context ID to contain generic information such as your institution's home page, which is then used as the target page.

See:

- Provisioning Access Through the Gatekeeper
- Setting Up New User Registration Context
- Deploying New User Registration

New User Registration Web Service Operations

The New User Registration framework provides the SCC_USERREG service. The SCC_USERREG service includes the following service operations that are described in this section:

- SCC_USERREG_CREATEACCT—creates a user account.
- SCC_USERREG_AUTHENTICATE—authenticates a user.
- SCC_USERREG_GET_USERID—retrieves the user ID.
- SCC_USERREG_GET_PSWD_HINT—retrieves the password hint.
- SCC_USERREG_GET_PASSWORD—resets user password.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

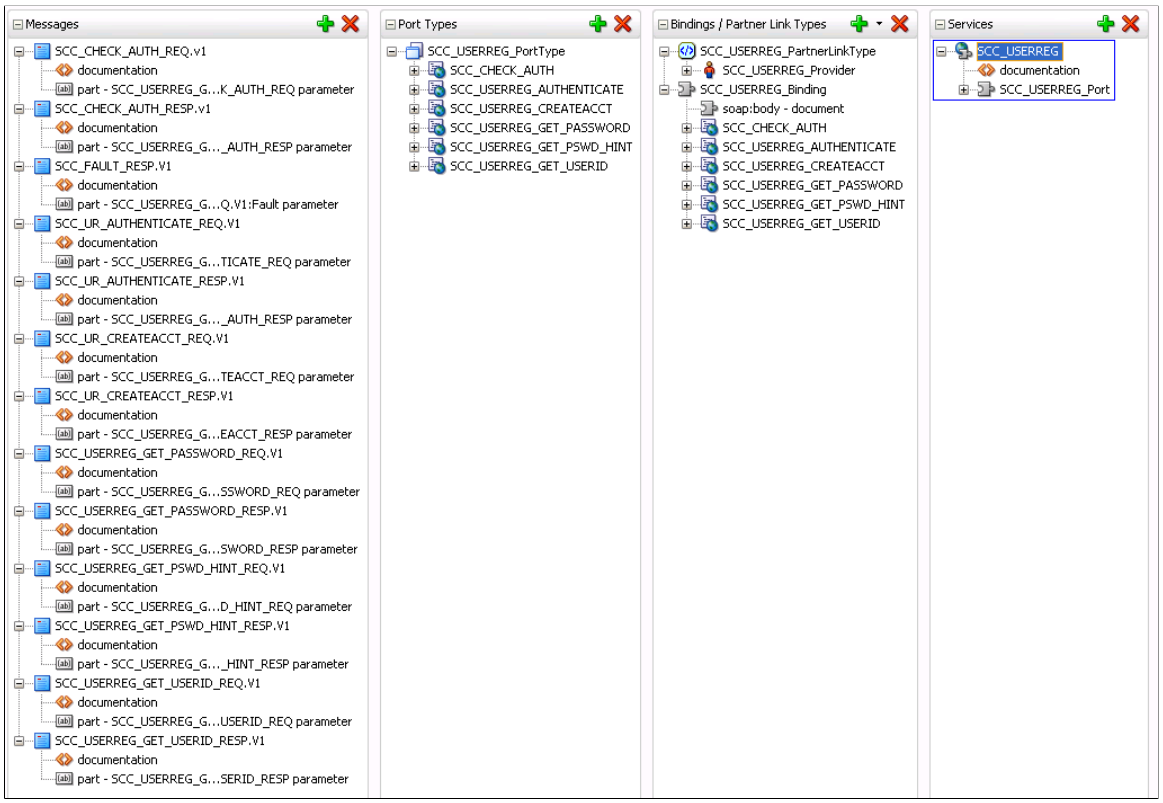
- SCC_CHECK_AUTH—authenticates a user, and checks if the user has the required security role (authorization)

Note: If a SOAP service request XSD contains the 'languageCd' parameter then the service is enabled for National Language Support (NLS). An ISO Locale value must be passed as the languageCd variable. Valid values can be found in PeopleTools, Utilities, International, Languages.

The following diagram shows the SCC_USERREG web service operations and their messages. The diagram also shows the location from where an online transaction can access the SCC_USERREG web service.

Image: SCC_USERREG Web Services and Locator Example

This example illustrates the fields and controls on the SCC_USERREG Web Services and Locator Example. You can find definitions for the fields and controls later on this page.



Create User Account (SCC_USERREG_CREATEACCT) Service Operation

Use this service operation to enable an online user to create a user name (user ID) and password. This service operation creates a new PeopleTools user profile.

The service operation supports the PeopleTools user management system. The service operation also supports other user management systems through the adapter architecture. To allow your PeopleSoft system to interact with another user management system through SCC_USERREG, a new adapter must be created.

When calling the Create User Account service operation, the user is required to choose a user name and password, and optionally to enter some constituent information such as first name, last name, email

 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

address, and so on. This either creates or does not create a single user account in the user management system you configure. If the user name is valid and does not already exist in the user management system, the service operation creates a user account. The new user account can be used immediately (no need for the new user to manually login). The user account is created based on an existing user ID that serves as a template (the SCC_SS_TEMPLATE user ID). This account must contain the basic role and permission security to access and use your system. This is also referred as the generic role provisioning. The service operation copies the user default information contained in this template, to create the new account. Therefore, you must set up the SCC_SS_TEMPLATE user account to allow an online transaction to use New User Registration. A second user ID that needs to be created and which also serves as a template to create user profiles is SCC_GUEST.

See Developer Reference to Deploy New User Registration, “Step 1: Initial Setup for New User Registration.”

The Create User Account service operation:

1. Verifies whether the required input parameters have been passed in the user registration page (user name, password, and confirm password).
2. Retrieves any constituent information from the input parameters, if included in the registration page, and validates the information. The constituent information is stored in the CTM constituent staging tables using the CTM transaction NEW_USER_REGISTRATION.
3. Calls the user management adapter to:
   a. Verify that the requested user name does not exist in the user management system.
   b. Verify your Password Controls setup is respected. This is defined in PeopleTools, Security, Password Configuration, Password Controls.
   c. Create the new user account.
   d. Authenticate the user and signs the user into the online transaction.
4. Prepares the response message. The service operation either creates a new user account which the user can immediately use or returns an error. The service error returns an error in the following conditions:
   - User name, password or confirm password input parameters are invalid.
   - Constituent information provided through the input parameters is invalid.
   - The PeopleSoft Password Controls rules are not respected.
   - An account for the same user name already exists in the user management system.

Note: If you intend to use the Forgot User ID and Forgot Password utilities, you must require the user to enter an email address when they create an account. To do this, you must select the Email Address check box in the New User Registration Installation page. The email address the user provides is stored in the newly created user profile and serves to send user ID or reset password if the user later forgets his or her user ID or password. The New User Registration sample login page and New User Registration Tester page are integrated with the Forgot User ID and Forgot Password utilities. To take advantage of this integration, make sure you select the Email Address check box in the New User Registration Installation page.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

See Defining Installation Options for New User Registration.

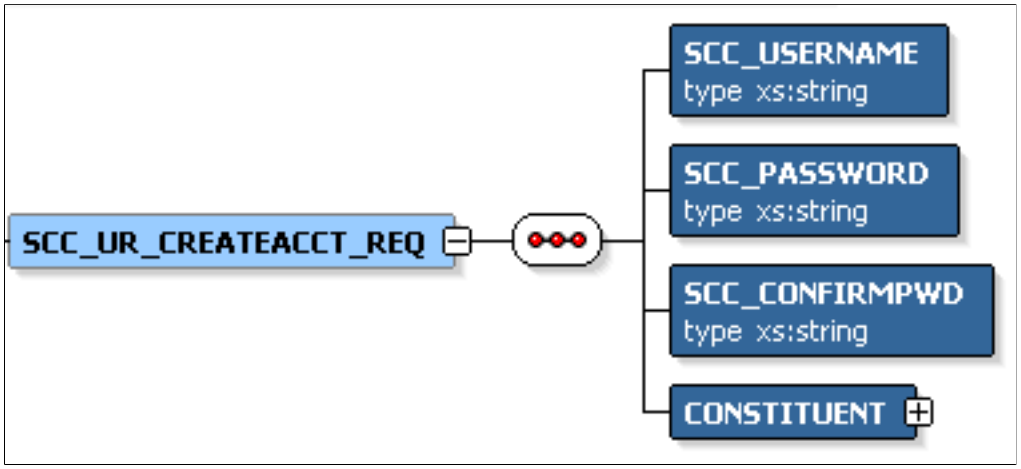
The Create User Account service operation includes the following three messages:

Input message: SCC_UR_CREATEACCT_REQ

The following diagram shows the input parameters that the SCC_USERREG_CREATEACCT service operation receives from a calling online transaction (mostly the user registration page):

Image: SCC_UR_CREATEACCT_REQ Message Parameters

This example illustrates the fields and controls on the SCC_UR_CREATEACCT_REQ Message Parameters. You can find definitions for the fields and controls later on this page.



The following input parameters are mandatory by the registration page to pass to the service operation:

- SCC_USERNAME
- SCC_PASSWORD
- SCC_CONFIRMPWD
- CONSTITUENT

While the CONSTITUENT tag is required in the request message (as indicated in the request message schema: <xs:element maxOccurs="1" minOccurs="1" ref="CONSTITUENT"/>) the CONSTITUENT elements can be empty in the request. This is because it is possible, but optional to gather constituent information at registration time.

Constituent is an entity defined in the Entity Registry. Use the PeopleTools Schema page to access the SCC_ENTITY_CONSTITUENT message schema (PeopleTools, Integration Broker, Integration Setup, Messages, Schema). Any attributes contained in the schema can be used in the registration page.

See Setting Up Entity Registry.

The following is an example of the SCC_UR_CREATEACCT_REQ message that the SCC_USERREG_CREATEACCT service operation receives from a user registration page:

```
<?xml version="1.0"?>
<SCC_UR_CREATEACCT_REQ>
        <SCC_USERNAME>KANGA</SCC_USERNAME>
        <SCC_PASSWORD>Rooly23</SCC_PASSWORD>
        <SCC_CONFIRMPWD>Rooly23</SCC_CONFIRMPWD>
```

 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

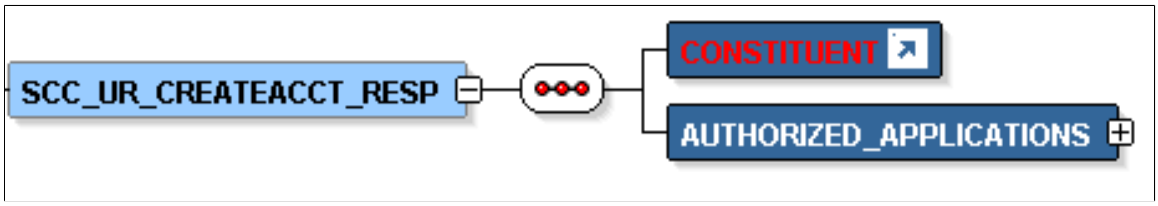
```
  <CONSTITUENT>
   <!-- Constituent data shape -->
  </CONSTITUENT>
</SCC_UR_CREATEACCT_REQ>
```

Output message: SCC_UR_CREATEACCT_RESP

The following diagram shows the output parameters that the SCC_USERREG_CREATEACCT service operation passes to the calling online transaction:

Image: SCC_UR_CREATEACCT_RESP Message Parameters

This example illustrates the fields and controls on the SCC_UR_CREATEACCT_RESP Message Parameters. You can find definitions for the fields and controls later on this page.



Constituent is an entity defined in the Entity Registry. Use the PeopleTools Schema page to access the SCC_ENTITY_CONSTITUENT schema (PeopleTools, Integration Broker, Integration Setup, Messages, Schema).

Image: Example of the SCC_UR_CREATEACCT_RESP message that the SCC_USERREG_CREATEACCT service operation responds to the calling online transaction

This example illustrates the fields and controls on the Example of the SCC_UR_CREATEACCT_RESP message that the SCC_USERREG_CREATEACCT service operation responds to the calling online transaction. You can find definitions for the fields and controls later on this page.

```
<?xml version="1.0"?>
<SCC_UR_CREATEACCT_RESP>
        <CONSTITUENT>
                <!-- Constituent data shape -->
        </CONSTITUENT>
        <NUR_REGISTRATION_CONTEXT>
                <SCC_APPL_CONTXT_ID>SCC_NURCTXT_20120918102441</SCC_APPL_CONTXT_ID>
                <SCC_APPL_CONTEXT>NUR_DELEGATED_ACCESS</SCC_APPL_CONTEXT>
                <URL>http%3a%2f%2fyourKioskServer.yourKioskDomain.com%2fpsc%2fyourCSPSoftWebsiteName%
                2fEMPLOYEE%2fHRMS%2fc%2fSCC_NUR.SCC_NUR_REG.GBL%3dstart%3fCAMPUS_URL%3dhttp%253a%
                252f%252fyourCSServerName.yourCSDomainName%252fpsc%252fyourCSPSoftWebsiteName%
                252fEMPLOYEE%252fHRMS%252fs%252fWEBLIB_SCC_NUR.SCC_SS_GATEKEE
                PER.FieldFormula.IScript_SCC_GateKeeper%253fSCC_APPL_CONTXT_ID%253dSCC_NURCTXT_
                20120918102441</URL>
        </NUR_REGISTRATION_CONTEXT>
</SCC_UR_CREATEACCT_RESP>
```

Fault message: SCC_FAULT_RESP

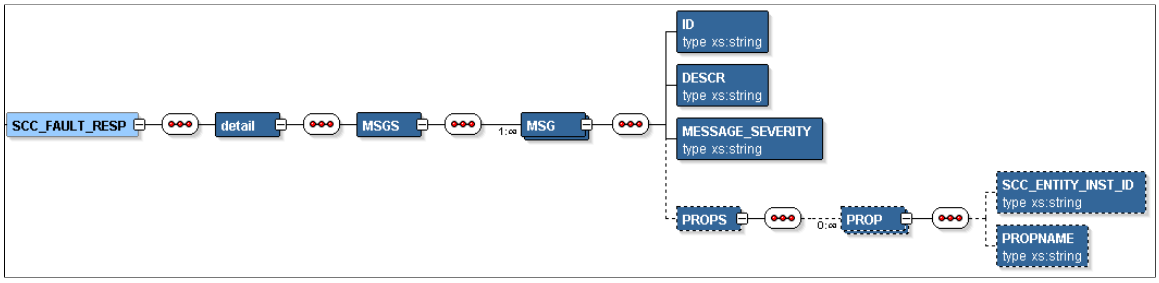
If the service operation encounters an error condition, it responds with the SCC_FAULT_RESP message.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The following diagram shows the output parameters that the SCC_FAULT_RESP service operation passes to the calling online transaction:

Image: SCC_FAULT_RESP Message Parameters

This example illustrates the fields and controls on the SCC_FAULT_RESP Message Parameters. You can find definitions for the fields and controls later on this page.



Authenticate User (SCC_USERREG_AUTHENTICATE) Service Operation

This service operation uses the delivered User Manager adapter to validate a username (user ID) and password combination with the installed user management system. The service operation is delivered with the ability to authenticate a user using the PeopleTools user management system.

A call to the SCC_USERREG_AUTHENTICATE service operation verifies whether the supplied username and password combination is correct using the configured user management system. If the username and password combination is correct, then the user is signed into the PeopleSoft system. All users accessing the SCC_USERREG_AUTHENTICATE operation have an Anonymous status until they have been successfully authenticated. Anonymous users only have minimal system access.

Use SCC_USERREG_AUTHENTICATE to allow a user to access your system through a front door, such as a login page.

The Authenticate User (SCC_USERREG_AUTHENTICATE) service operation:

1. Verifies whether the input parameters exist (user name and password).
2. Calls the user management adapter to validate the user name and password combination.
3. If an EMPLID is tied to the retrieved user profile, uses the EMPLID to retrieve constituent information on the authenticated person.
4. Prepares the response message. The service operation either signs in the user to the PeopleSoft system or returns an error. The service error returns an error in the following conditions:
   - Input parameters, username and password, are invalid.
   - User name and password combination cannot be authenticated using the user management system.

The Authenticate User service operation includes the following messages:

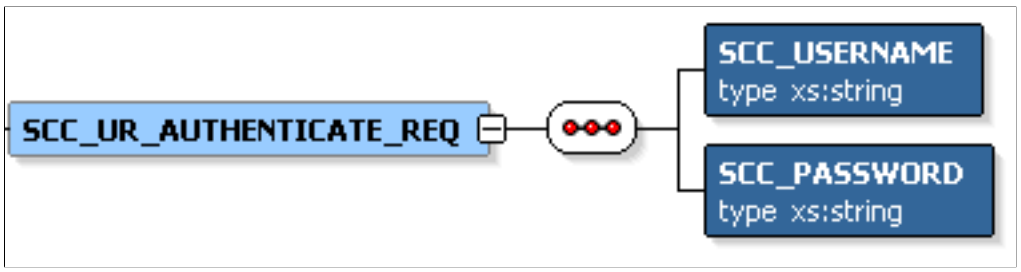
 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Input message: SCC_UR_AUTHENTICATE_REQ

The following diagram shows the input parameters that the SCC_USERREG_AUTHENTICATE service operation receives from a calling online transaction (mostly the user login page):

Image: SCC_UR_AUTHENTICATE_REQ Message Parameters

This example illustrates the fields and controls on the SCC_UR_AUTHENTICATE_REQ Message Parameters. You can find definitions for the fields and controls later on this page.



The following input parameters are mandatory for the login page to pass to the service operation:

- Username
- Password

The following is an example of the SCC_UR_AUTHENTICATE_REQ message that the SCC_USERREG_AUTHENTICATE service operation receives from a login page:

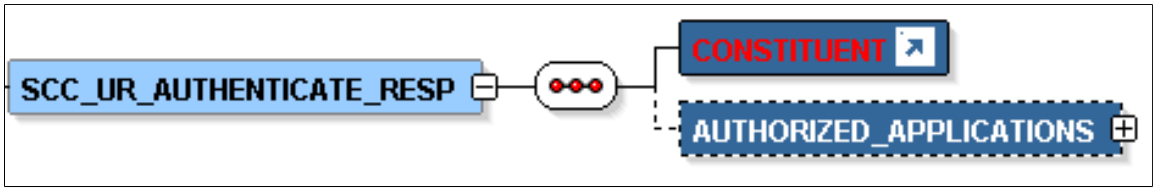
```
<?xml version="1.0"?>
<SCC_UR_AUTHENTICATE_REQ>
        <SCC_USERNAME>KANGA</SCC_USERNAME>
        <SCC_PASSWORD>Rooly23</SCC_PASSWORD>
</SCC_UR_AUTHENTICATE_REQ>
```

Output message: SCC_UR_AUTHENTICATE_RESP

The following diagram shows the output parameter that the SCC_USERREG_AUTHENTICATE service operation passes to the calling online transaction:

Image: SCC_UR_AUTHENTICATE_RESP Message Parameters

This example illustrates the fields and controls on the SCC_UR_AUTHENTICATE_RESP Message Parameters. You can find definitions for the fields and controls later on this page.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Constituent is an entity defined in the Entity Registry. Use the PeopleTools Schema page to access the SCC_ENTITY_CONSTITUENT schema (PeopleTools, Integration Broker, Integration Setup, Messages, Schema).

Image: Example of the SCC_UR_ AUTHENTICATE_RESP message that the SCC_USERREG_AUTHENTICATE service operation transmits to the calling online transaction

This example illustrates the fields and controls on the Example of the SCC_UR_ AUTHENTICATE_RESP message that the SCC_USERREG_AUTHENTICATE service operation transmits to the calling online transaction. You can find definitions for the fields and controls later on this page.

```
<?xml version="1.0"?>
<SCC_UR_AUTHENTICATE_RESP>
    <CONSTITUENT>
        <!-- Constituent data shape -->
    </CONSTITUENT>
    <NUR_REGISTRATION_CONTEXT>
    <SCC_APPL_CONTXT_ID>SCC_NURCTXT_20120918102441</SCC_APPL_CONTXT_ID>
    <SCC_APPL_CONTEXT>NUR_DELEGATED_ACCESS</SCC_APPL_CONTEXT>
    <URL>http%3a%2f%2fyourKioskServer.yourKioskDomain.com%2fpsc%2fyourCSPSoftWebsiteName%2fEMPLOYEE%
      2fHRMS%2fc%2fSCC_NUR.SCC_NUR_REG.GBL%3dstart%3fCAMPUS_URL%3dhttp%253a%252f%
      252fyourCSServerName.yourCSDomainName%252fpsc%252fyourCSPSoftWebsiteName%252fEMPLOYEE%
      252fHRMS%252fs%252fWEBLIB_SCC_NUR.SCC_SS_GATEKEEPER.FieldFormula.IScript_SCC_GateKeeper%
      253fSCC_APPL_CONTXT_ID% 253dSCC_NURCTXT_20120918102441</URL>
    </NUR_REGISTRATION_CONTEXT>
</SCC_UR_AUTHENTICATE_RESP>
```

```
<?xml version="1.0"?>
<SCC_UR_CREATEACCT_RESP>
  <CONSTITUENT>
   <!-- Constituent data shape -->
  </CONSTITUENT>
<NUR_REGISTRATION_CONTEXT>
  <SCC_APPL_CONTXT_ID>SCC_NURCTXT_20120918102441</SCC_APPL_CONTXT_ID>
   <SCC_APPL_CONTEXT>NUR_DELEGATED_ACCESS</SCC_APPL_CONTEXT>
   <URL>http://yourServer.yourDomain.com/EMPLOYEE/SCC_DA_PROXY/SS_CC_DA_TERMS_CON</⇒
URL>
</NUR_REGISTRATION_CONTEXT>
</SCC_UR_CREATEACCT_RESP>
```

Fault message: SCC_FAULT_RESP

Refer to the SCC_FAULT_RESP message example in the SCC_USERREG_CREATEACCT service operation section.

Retrieve User ID (SCC_USERREG_GET_USERID) Service Operation

This service operation retrieves a user's ID using the Forgot User ID utility. A user must provide the email address that is associated with his or her OPRID (stored inside the user's profile) in order to retrieve the user ID. The user ID is retrieved only if one OPRID is associated with the email address. The New User Registration framework uses the Notifications framework to generate the email message that contains the user ID.

The Retrieve User ID service operation:

1. Verifies whether the required input parameter (email address) has been passed to the Forgot my User ID page.
2. Validates whether the email address entered is associated with only one user ID (OPRID) (from the PSOPRDEFN and PSUSEREMAIL records).

 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

3. Prepares the response message. The service operation either retrieves the user ID and uses the Notifications framework to send an email that contains the user ID, or returns an error. An error is returned when:
   - The email address is not found.
   - The email address is associated with multiple user IDs (OPRIDs), or to no user ID.

See Notifications Framework and New User Registration.

The Retrieve User ID service operation includes the following messages:

Input Message: SCC_USERREG_GET_USERID_REQ

The email address is a mandatory input parameter to pass to the service operation. The utility evaluates whether there is only one OPRID assigned to the email address. If so, the user ID is retrieved.

Output Message: SCC_USERREG_GET_USERID_RESP

When the user ID is retrieved, an email that contains the user ID is sent to the user as part of the response. The Notifications framework is triggered to send the email message.

If more than one user ID is assigned to an email address or no user ID is found, the user ID is not retrieved and an error message appears.

See:

- Using the Forgot User ID Utility
- Step 9: Configuring the Forgot User ID Utility

Retrieve Password Hint (SCC_USERREG_GET_PSWD_HINT) Service Operation

This service operation retrieves the Forgot Password Hint set when a user forgets his or her password and triggers the PeopleTools Forgot Password utility. The PeopleTools Forgot Password utility requires that Forgot Password Hints should be defined. A user must provide his or her user ID in order to reset and receive a new password. When a user forgets his or her password and invokes the Forgot Password utility, the user ID that is provided is used to fetch the email address and Forgot Password hint set. The user's response is compared with the information stored in the database.

The Retrieve Password Hint service operation:

1. Verifies whether the required input parameter, user ID (OPRID), has been passed in the Forgot my password page.
2. Evaluates whether the user ID is valid.
3. Prepares the response message. If the user ID is valid, the service operation retrieves the associated email address and displays the password hint set, or returns an error. An error is returned when:
   - The user ID is not found.
   - The user ID is not associated with a Forgot Password hint set.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

- The user ID is not associated with an email address, so an email cannot be sent.

See Using the Forgot Password Utility.

The Retrieve Password Hint service operation includes the following messages:

Input Message: SCC_USERREG_GET_PSWDHINT_REQ

The user ID (OPRID) is a mandatory parameter to pass to the service operation. The service operation evaluates whether the user ID is valid. If so, the associated email address and hint question are retrieved.

Output Message: SCC_USERREG_GET_PSWDHINT_RESP

If the user ID is valid, the associated email address and hint question are returned. If the user ID does not exist, is not associated with an email address or hint question, the service operation displays an error.

See Developer Reference to Deploy New User Registration, “Step 10: Configuring the Forgot Password Utility.”

Reset Password (SCC_USERREG_GET_PASSWORD) Service Operation

This service operation resets a user’s password using the PeopleTools Forgot Password utility. When a user forgets his or her password and uses the Forgot Password utility, the user ID that is provided is used to fetch the associated Forgot Password hint set. The user must provide the correct response to the hint question. The response is compared with the information stored in the database, and when the information matches, a new password is generated and emailed to the user.

The Reset Password service operation:

1. Evaluates whether the user’s response to the hint question matches the information stored in the database.
2. Generates a new password if the user’s response and the information in the database match.

The Reset Password service operation includes the following messages:

Input Message: SCC_USERREG_GET_PASSWORD_REQ

The hint response is a mandatory parameter to pass to the service operation. The custom interface SCC_NUR_EMAIL_PSWD is invoked. If the hint response matches the information in the database, the password is reset and all the PeopleTools tables are updated with the new password.

Output Message: SCC_USERREG_GET_PASSWORD_RESP

A new password is generated and emailed to the user through the PeopleTools Forget Password email utility.

Check Authorization (SCC_CHECK_AUTH) Service Operation

This service operation uses the User Manager adapter to validate a user name (user ID) and password combination against your user management system. The service operation provides an additional facility

 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

to return authorization information for an authenticated user. The service operation also authenticates a user using the PeopleTools user management system.

A call to the SCC_CHECK_AUTH service operation verifies whether the supplied user name and password combination is correct using the configured user management system. If the user name and password combination is correct, then the user is signed into the PeopleSoft system. Optionally, this service operation can return Role Based Access control (RBAC) authorization information for the authenticated user. The service caller can include optional role filter criteria in the request. The optional role filter criteria is compared against the PeopleSoft RBAC information associated with the user profile, and the matching role information is then returned to the client. This means that the user has access to the returned roles. All users accessing the SCC_CHECK_AUTH operation have an Anonymous status until they have been successfully authenticated. Anonymous users only have minimal system access.

Use SCC_CHECK_AUTH to allow a user to access your system through a front door, such as a login page, and to validate role authorization information.

The Check Authorization service operation:

1. Verifies whether the input parameters exist (user name and password and optional Role filters).
2. Calls the user management adapter to validate the user name and password combination.
3. Matches the roles to the user profile roles and returns *only* roles that are common, if the optional role filters are provided.
4. Prepares the response message. The service operation either signs in the user to the PeopleSoft system or returns an error. An error is returned when:
   - The input parameters, user name and password, are invalid.
   - The user name and password combination cannot be authenticated using the user management system.

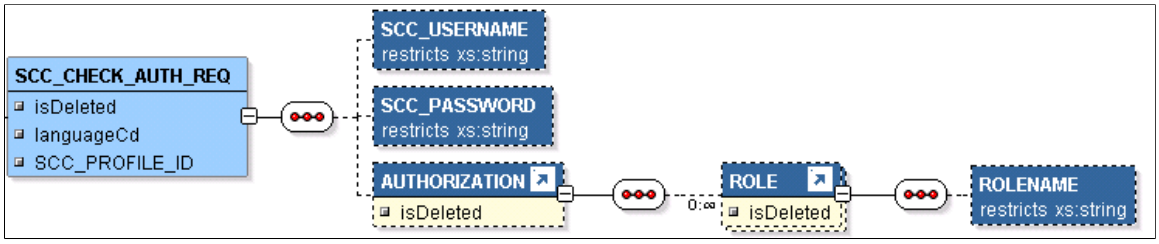
The Check Authorization User service operation includes the following messages:

Input message: SCC_CHECK_AUTH_REQ

The following diagram shows the input parameters that the SCC_CHECK_AUTH service operation receives from a calling online transaction. For example, the user login page:

Image: SCC_CHECK_AUTH_REQ Message Parameters

This example illustrates the fields and controls on the SCC_CHECK_AUTH_REQ Message Parameters. You can find definitions for the fields and controls later on this page.



The following input parameters are mandatory for the login page to pass to the service operation:

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

- User name
- Password

The following is an example of the SCC_CHECK_AUTH_REQ message that the SCC_CHECK_AUTH service operation receives from a login page:

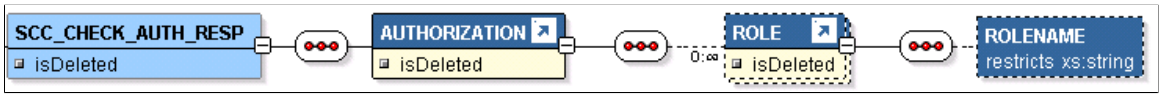
```
<?xml version="1.0"?>
<SCC_CHECK_AUTH_REQ>
 <SCC_USERNAME>KANGA</SCC_USERNAME>
 <SCC_PASSWORD>Rooly</SCC_PASSWORD>
  <AUTHORIZATION>
   <ROLE>
    <ROLENAME>CS - Prospect</ROLENAME>
    <ROLENAME>CS - Student</ROLENAME>
   </ROLE>
<  /AUTHORIZATION>
</SCC_CHECK_AUTH_REQ>
```

Output message: SCC_CHECK_AUTH_RESP

The following diagram shows the output parameter that the SCC_CHECK_AUTH service operation passes to the calling online transaction:

Image: SCC_CHECK_AUTH_RESP Message Parameters

This example illustrates the fields and controls on the SCC_CHECK_AUTH_RESP Message Parameters. You can find definitions for the fields and controls later on this page.



The following is an example of the SCC_CHECK_AUTH_RESP message that the SCC_CHECK_AUTH service operation transmits to the calling online transaction:

```
<?xml version="1.0"?>
<SCC_CHECK_AUTH_RESP xmlns="http://xmlns.oracle.com/Enterprise/services">
 <AUTHORIZATION>
  <ROLE>
   <ROLENAME>CS - Student</ROLENAME>
  </ROLE>
 </AUTHORIZATION>
</SCC_CHECK_AUTH_RESP>
```

Fault message: SCC_FAULT_RESP

See Create User Account (SCC_USERREG_CREATEACCT) Service Operation, Fault message: SCC_FAULT_RESP.

Using the New User Registration Sample User Interfaces

This section describes the New User Registration sample pages and discusses the:

- New User Registration login sample page.
- New User Registration Tester page.
- User Flow for a returning user

 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

- User Flow for a guest
- Forgot User ID Utility.
- Forgot Password Utility.

The New User Registration sample login pages are visually similar. These pages allow a user to create a new user account or use an existing account to access your system. These pages are meant to be used only as a reference or guide for implementing New User Registration in your institution. The sample login page serves as an example of how your own custom (institution-specific) login page can be integrated and deployed with New User Registration. The sample page works only with the Kiosk setup. For example, it can reside outside of your firewall and be set up as a kiosk.

The New User Registration Tester page is used for testing purposes such as evaluating the security objects that comprises the New User Registration framework. The Tester page contains the same functionality included in the New User Registration login sample page (except the Autologger and Gatekeeper), but is meant to be used in the same database. The Tester page is intended to be used *only* for testing purposes.

While both sample login pages are visually similar, the New User Registration sample login page is fully integrated with all the delivered New User Registration framework security objects in order to:

- Provision the basic roles set up in SCC_SS_TEMPLATE.
- Trigger the New User Registration web service operations for creating and authenticating a user (SCC_USERREG_CREATEACCT and SCC_USERREG_AUTHENTICATE).
- Use the delivered New User Registration CTM transaction (NEW_USER_REGISTRATION).
- Take advantage of the New User Registration Context ID.
- Validate user authorization and authentication based on PeopleTools security.
- Allow a user to launch the Forgot User ID or Forgot Password utility.

You can deploy New User Registration fully or partially, or if you already have your own security management system, you can continue to use it.

Note: The New User Registration sample login pages are not intended to be deployed in a production environment for end users.

Pages Used to Access New User Registration Sample User Interfaces

Page Name	*Definition Name*	*Navigation*	*Usage*
New User Registration	SCC_NUR_REG	Set Up SACR, System Administration, Utilities, Sample User Interfaces, New User Registration	Shows an example of how to integrate and deploy your custom login page with New User Registration.
New User Registration Tester	SCC_NUR_TESTER	Set Up SACR, System Administration, Utilities, Sample User Interfaces, New User Registration Tester	Tests and evaluates New User Registration framework objects.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Page Name	*Definition Name*	*Navigation*	*Usage*
Forgot my User ID	SCC_NUR_FRGT_USRID	Click the Forgot your User ID link on the New User Registration or New User Registration Tester page.	Retrieves user ID.
Forgot My Password	SCC_NUR_FRGT_PSWD	Click the Forgot your password link on the New User Registration or New User Registration Tester page.	Resets user password.

Using the New User Registration Login Sample Page

The New User Registration login sample page is also integrated with the following New User Registration framework security objects:

- The Autologger to immediately sign in the user into your system.
- The Gatekeeper to optionally provision specific application role level security and to transfer to an application specific target page.
- A specific or defaulted New User Registration Context ID specified in the URL to access your login sample page.
- The language links to access your system in the user's preferred language (requires that your system supports translation for at least one language other than the base language).

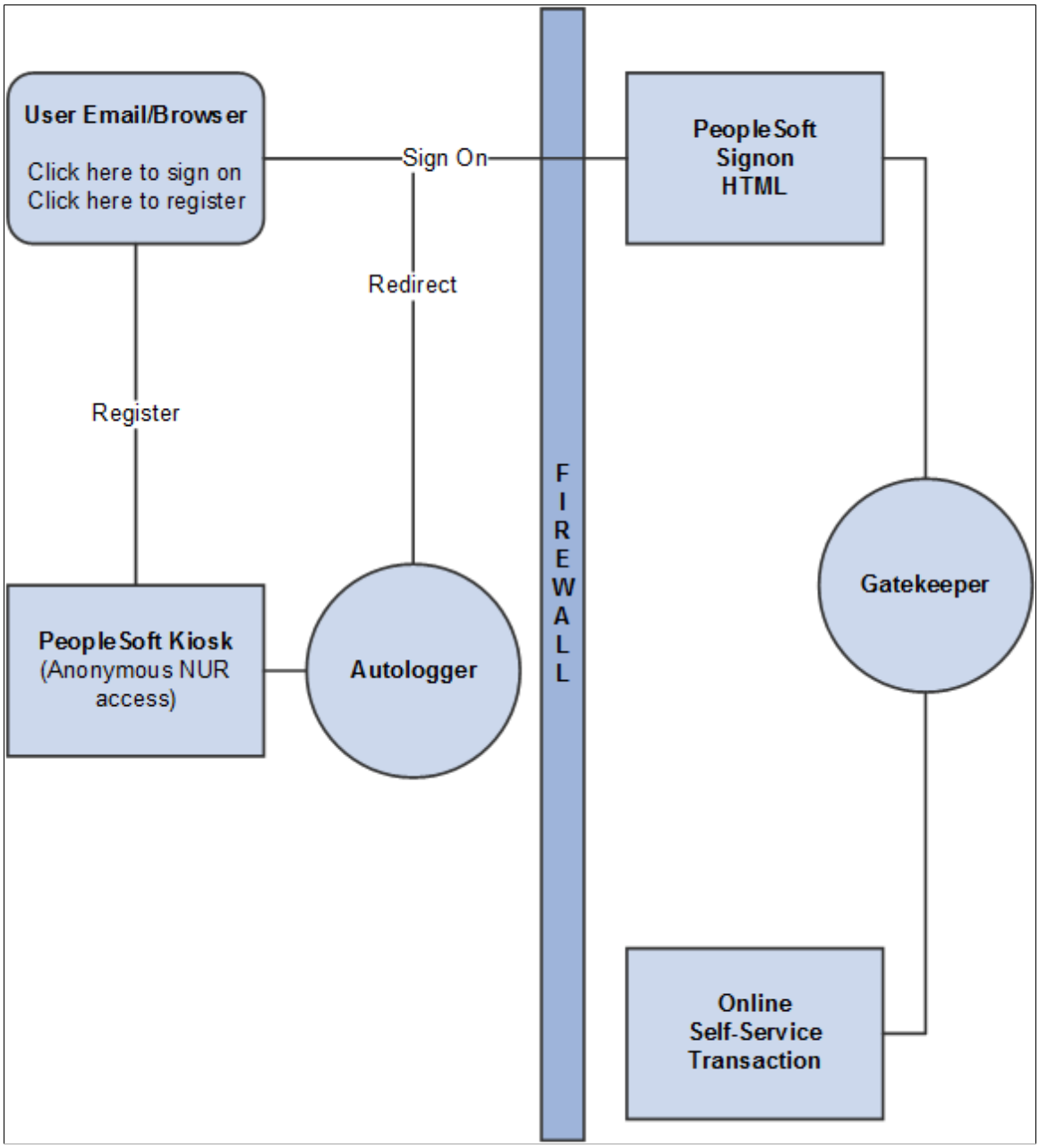
The New User Registration login sample page is intended to be used outside of your system firewall, for example within a Kiosk. When the page is deployed, the login page (or a custom version of it) is accessed through a URL (not from a Peoplesoft regular menu navigation). The URL is embedded with the Gatekeeper information and, optionally, a New User Registration Context ID.

 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The following diagram shows how the login sample page deployed with a Kiosk can be represented:

Image: Deployment Example of New User Registration login sample page

Deployment Example of New User Registration login sample page



The self service Kiosk allows anonymous users access to the New User Registration page outside the firewall.

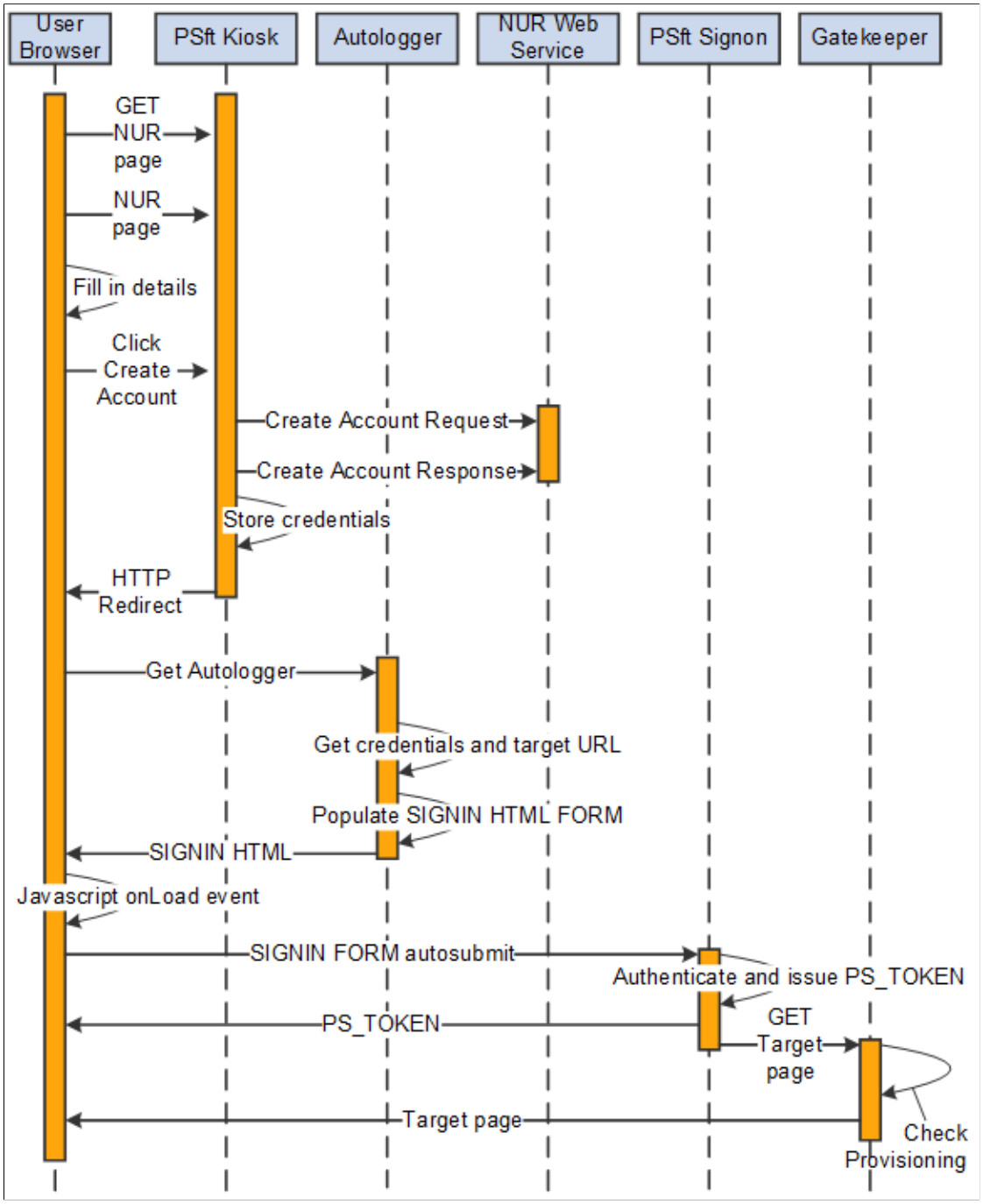
After an account is created, a user is authenticated via the standard PeopleTools login page. To allow for a seamless experience, the Autologger facilitates the automatic sign-on after account creation. In the case of

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

account creation, the embedded URL (CAMPUS_URL) is used to retain information on the target page. The following diagram shows the orchestration and flow between the various components:

Image: Orchestration of various New User Registration framework elements

Orchestration of various New User Registration framework elements



All sign-in related request and response processing should occur over a secure transport layer (SSL) until such a point as the PS_TOKEN cookie is issued to the browser.

 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Using the New User Registration Tester Page

The New User Registration Tester page is visually similar to the New User Registration login sample page, but has the following use and implementation differences:

- The page is deployed within your firewall (resides inside the production database). It is only for testing and evaluating the New User Registration framework. Your developers should use the tester page to review and understand the different pieces contained in the New User Registration framework.
- It is accessed by a system administrator (not by an end user) from a PeopleSoft menu navigation, not from a URL.
- The Autologger is replaced by the SwitchUser function. Because the page is contained in your system database and is accessed by a system administrator, the SwitchUser function signs off the administrative user ID to sign in the newly created user ID or the existing user ID you enter in the login page.
- Because a URL is not used, a New User Registration context ID is not specified. Instead, the New User Registration Tester page uses the New User Registration context ID you set with the Default field checked.
- Clicking the displayed language links do not change the language in which the newly created user or the returning user sees the system. Because the New User Registration Tester is first accessed by the system administrator, the SwitchUser function does not change the languages.

Note: The tester page is intended for testing purposes and should *not* be deployed in a production environment.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

User Flow For a Returning User

1. Navigate to the New User Registration Tester page or access the New User Registration login sample page from a predefined URL.

   Image: New User Registration login sample page or Tester page

   This example illustrates the fields and controls on the New User Registration login sample page or Tester page. You can find definitions for the fields and controls later on this page.

User ID	Provide an existing user ID.
Password	Provide the password.
Sign In	Click to sign into the system. The system validates whether the user ID and password match a valid user profile. If the validation passes without errors, the system triggers the SCC_USERREG _AUTHENTICATE service operation, auto logger, and gatekeeper.
Select a Language	Displays the list of languages supported by your system. The guest can select a language from this list in which he or she can view and use the PeopleSoft system, as well as locale formatting conventions for dates, times, and number.
Forgot your User ID	Click to access the Forgot my User ID page.
Forgot your password	Click to access the Forgot My Password page.

2. The returning user enters the user ID and password, and clicks the Sign In button. This triggers the SCC_USERREG_AUTHENTICATE service operation, auto logger (or SwitchUser if the New User Registration Tester page is used) and gatekeeper.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

3. If the New User Registration login sample page is used, the new user is authenticated through the PeopleTools security logic to access your system. Because of that the user sees, for a few seconds, your regular login page pre-populated with the user ID and the password entered by the returning user. Below is an example of what the user sees if the delivered PeopleTools login page is used:

   Image: PeopleTools login page

   This example illustrates the fields and controls on the PeopleTools login page . You can find definitions for the fields and controls later on this page.

   Depending on how you deploy the user registration page, you may want to replace this page with a message such as, “Please be patient while we are transferring you to our system.” To customize the message, you modify the HTML found in the SCC_PT_SIGNON.HTML object in application designer, then replace the text with the message: *Please be patient while we are transferring you to our system.*

   You will view the main login page only when signing in through the New User Registration login sample page. If the New User Registration Tester page is used, you will not see it because the authentication is performed within the same database and you are signed into the system through the SwitchUser function.

4. After successful authentication, the returning user is automatically signed into the system. If a New User Registration Context ID is known (whether it is passed through a URL if the New User Registration login sample page is used or a default New User Registration Context ID is identified in the case of the New User Registration Tester page), and security role(s) are listed, the system provisions the application level security role(s) defined. If the New User Registration Context ID includes a target page, the system transfers the returning user directly to the target page. Else, the system transfers the returning user to the application client’s home page.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

User Flow For a Guest

1. Navigate to the New User Registration Tester page or access the New User Registration login sample page from a predefined URL. From these pages, the new user registration fields appear below the sign-in fields (under Create Account) and users without an existing user ID can directly register a new account.

   If the New User Registration login sample page is used, then after pressing the Create Account button, the new user is authenticated through the PeopleTools security logic to access your system. Because of that the user sees, for a few seconds, your regular login page pre-populated with the user ID and the password entered by the guest. Below is an example of what the user sees if the delivered PeopleTools login page is used:

   Image: PeopleTools login page

   This example illustrates the fields and controls on the PeopleTools login page . You can find definitions for the fields and controls later on this page.

   Depending on how you deploy the user registration page, you may want to replace this page with a message like: “Please be patient while we are transferring you to our system.” To customize the message, you modify the HTML found in the SCC_PT_SIGNON.HTML object in application designer, replace the text with the message: *Please be patient while we are transferring you to our system.*

   You see the main login page only when signing in through the New User Registration login sample page. If the New User Registration Tester page is used, you do not see it because the authentication is performed within the same database and you are signed into the system through the SwitchUser function.

2. Clicking the Create Account button triggers the SCC_USERREG_CREATEACCT service operation, auto logger (or SwitchUser if the New User Registration Tester page is used), and gatekeeper.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

3. After successful authentication, the new user is automatically signed into the system. If a New User Registration Context ID is known (whether it is passed through a URL if the New User Registration login sample page is used or a default New User Registration Context ID is identified in the case of the New User Registration Tester page), and security role(s) are listed, the system provisions the application level security role(s) defined. If the New User Registration Context ID includes a target page, the system transfers the new user directly to the target page. Else, the system transfers the new user to the application client's home page.

The following table describes the registration fields in the New User Registration login sample or Tester page:

Choose your User ID	Enter a user ID. Some institutions might prefer to create user IDs by prefixing some letters, using their own algorithm (for example, an institution named PeopleSoft University may want their user IDs to start with the letters PU). No such algorithm is delivered with this sample user interface. If required, institutions can add logic to their user interface for user ID creation.
Create a password and **Confirm your password**	Enter a password. The system performs the validation when the user clicks the Create Account button.
Email Address, First Name and **Last Name**	(Optional) Enter constituent information. If you select the Email Address check box in the New User Registration Installation page, you can require users to enter an email address. Although the SCC_USERREG_CREATEACCT service operation supports most of the constituent fields, the sample New User Registration login pages include only these three constituent fields. You can add more constituent fields if required, or remove fields if you do not want to gather constituent information at account creation time. The values that the guest enters in these constituent fields are stored in the constituent staging records. Additionally, the email address is also stored in the newly created user profile. The email address in the user profile is used in the Forgot User ID and Forgot Password utilities. Use the PeopleTools Schema page to access the SCC_ENTITY_CONSTITUENT schema (PeopleTools, Integration Broker, Integration Setup, Messages, Schema). Any attributes contained in the schema can be used in the registration page. The constituent information is stored in the CTM constituent staging tables and can be viewed using the Constituent Staging component under the CTM transaction code called NEW_USER _TRANSACTION. At this stage no EMPLID is assigned so the data cannot be promoted to the corresponding production tables. Staging the data allows retrieval from inside a subsequent CTM transaction. Because the subsequent transaction also stores the

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

data in the CTM constituent staging tables, the self-service user does not have to enter the same information twice. For example, during registration or while performing the subsequent CTM transaction.

See:

- Understanding New User Registration, “CTM and New User Registration”
- Understanding CTM
- Defining Installation Options for New User Registration

Create Account

Click to create your account.

The system verifies whether the:

- information in the Create a password and Confirm your password fields match. If they do not match, an error message appears.
- user ID exists in the PeopleTools security table (PSOPRDEFN record).
- information in the constituent fields is valid (for example, whether the email address is valid).

If the validation passes without errors, the system stores the constituent information in the CTM staging records and triggers the SCC_USERREG_CREATEACCT service operation.

Using the Forgot User ID Utility

Click the Forgot your User ID link on the New User Registration login sample page or New User Registration Tester page.

Enter your Email address

Provide an email address. This is used to retrieve the user ID (OPRID).

The email address you provide must match one and only one user ID in the system. If so, a successful message appears: *Your request was successful. Your User ID will be sent at the email address you entered.* If the email address is either associated to multiple user IDs or to no user ID, an error message appears: *We cannot retrieve your username at this time.*

Retrieve User ID

Click to validate the email address. If the process locates the email address inside a user profile, it triggers the Notifications Framework to send an email message that contains the user ID.

See Understanding the Notifications Framework.

Return to the logon page

Click to cancel the process and return to the login page.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Note: Before you deploy this functionality and to enable users to invoke the Forgot User ID utility, all user IDs in your system must have an associated email address in the user profile. If user IDs are created using the SCC_USERREG_CREATEACCT service operation, make sure users are required to provide an email address when they create an account. To require users to provide an email address, select the Email Address check box in the New User Registration Installation page. The email address is used to retrieve the user ID and to send the email notification message that includes the user ID. The delivered New User Registration login sample page and New User Registration Tester page require the email address field to be populated at account creation time. This ensures that user IDs created through New User Registration have an email address stored in the user profile.

Related Links

Developer Reference to Deploy New User Registration

Using the Forgot Password Utility

Click the Forgot your password link on the New User Registration login sample page or New User Registration Tester page.

User ID

Enter your user ID. This is used to retrieve the user's email address from the user's user profile so that the password can be regenerated and emailed to the user.

Continue

Click to access the Answer security question page.

When you click Continue, the system validates whether the user ID has an associated email address in the user profile. The email address is used to send the new password. If no email address is found, the following message is sent: *A new password cannot be sent as no email address was found. Contact your system administrator.*

Note: Before you deploy this functionality and to enable users to invoke the Forgot Password utility, all user IDs in your system must have an associated email address in the user profile. If user IDs are created using the SCC_USERREG_CREATEACCT service operation, make sure users are required to provide an email address when they create an account. To require users to provide an email address, select the Email Address check box in the New User Registration Installation page. The email address is used to retrieve the user ID and to send the email notification message that includes the user ID. The delivered New User Registration login sample page and New User Registration Tester page require the email address field to be populated at account creation time. This ensures that user IDs created through New User Registration have an email address stored in the user profile.

See Defining Installation Options for New User Registration.

Question

Shows the security question the user previously answered.

If a security question has not previously been answered, the user cannot reset his or her password. The following error message appears: *A security question has not previously been answered. Contact your system administrator.*

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

As delivered with the generic PeopleTools security, a self-service user can answer a security question by going to Home page, My System Profile. In the General Profile Information page, click the Change or set up forgotten password help link. The user can select a security question and enter a response. This page is delivered with your system and security needs to be granted to all of your users. Alternatively, a simpler self-service version of this page could be created.

Response

Enter the answer to the security question.

Email New Password

Click to trigger the email template utility and auto-generate a temporary password.

An email with a temporary password is sent only if the response to the security question is correct and there is an email address stored in the PSOPRDEFN.EMAILID field for the user ID that was provided. The password is automatically reset in the user's profile (in the PSOPRDEFN table).

The following is an example of an email message that might be sent to a user requesting his or her password to be reset:

You are receiving this auto-generated email message because you requested your Campus Solutions password to be resetted. Use the following temporary password: JMWFBUEU. Press this link or copy the below URL to access the system with your newly generated password. You will be requested to change the temporary password immediately. http://yourServer.yourDomain.com/psp/ps/EMPLOYEE/HRMS/s/WEBLIB_SCC_NUR.SCC_SS_GATEKEEPER.FieldFormula.IScript_SCC_GateKeeper?SCC_APPL_CONTEXT=SCC_NURCTXT_20130211110717

See Developer Reference to Deploy New User Registration, "Step 10: Configuring the Forgot Password Utility."

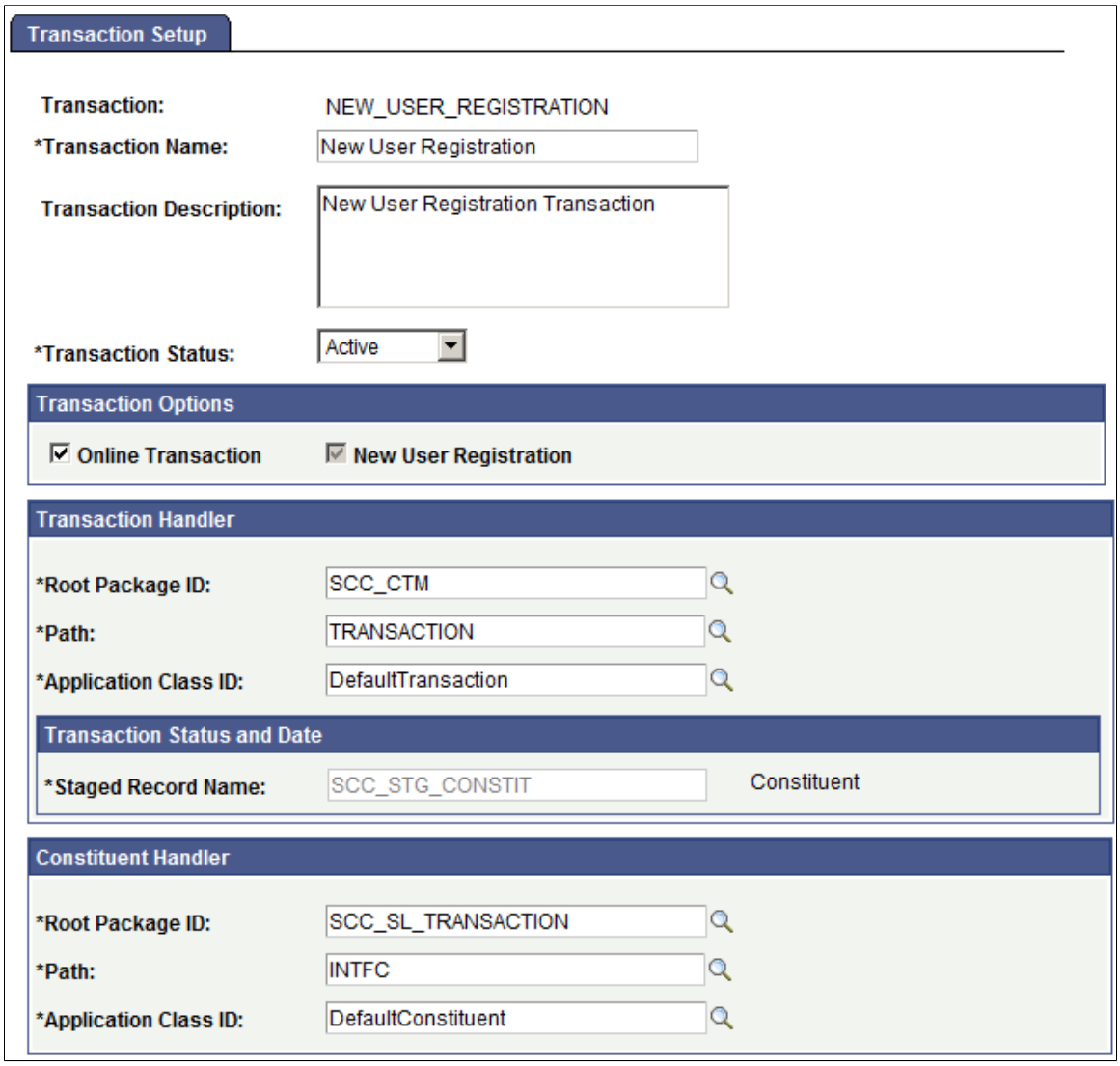
 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Setting Up CTM for New User Registration

Access the Transaction Setup page (Set Up SACR, System Administration, Utilities, Constituent Transaction Mgmt, Transaction Setup).

Image: Transaction Setup page - New User Registration

This example illustrates the fields and controls on the Transaction Setup page - New User Registration. You can find definitions for the fields and controls later on this page.



A New User Registration CTM transaction called NEW_USER_REGISTRATION is delivered with your system.

Verify the delivered and recommended setup for this transaction by accessing the CTM Transaction Setup page.

See Setting Up CTM, “Setting Up a Transaction.”

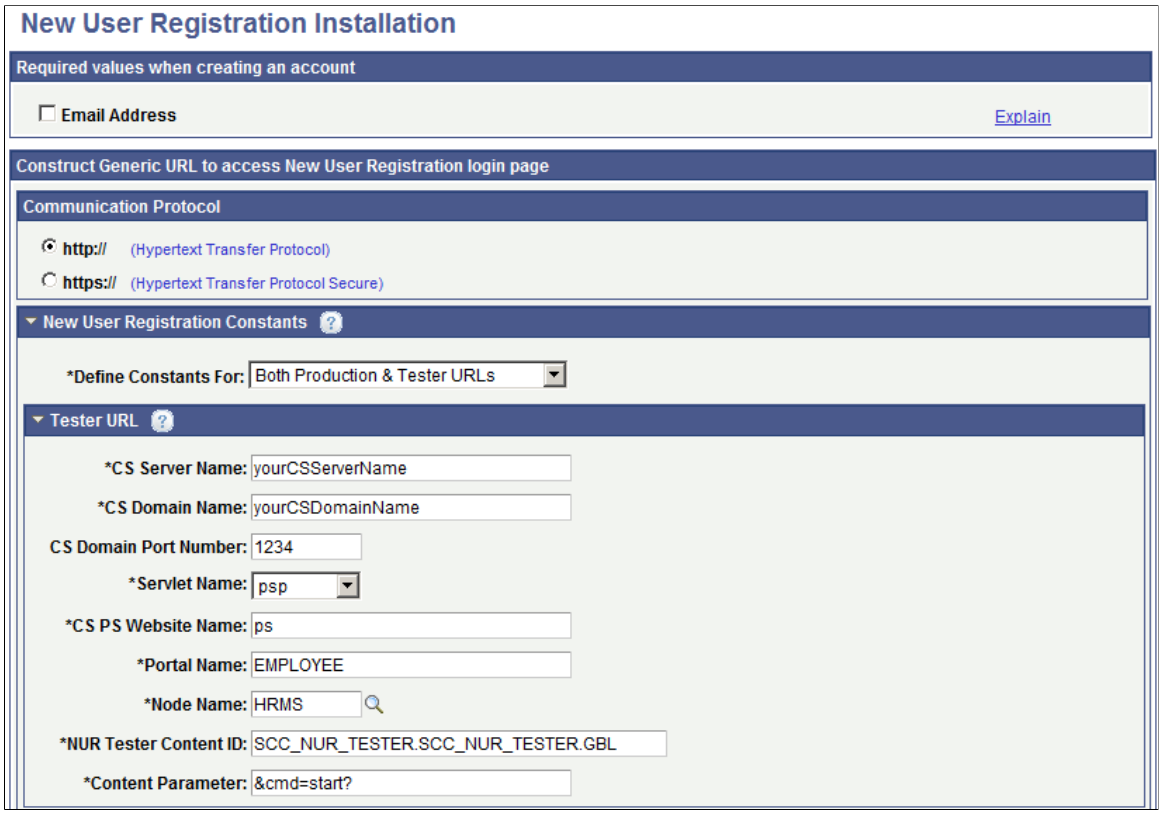
Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Defining Installation Options for New User Registration

Access the New User Registration Installation page (Setup SACR, System Administration, Utilities, New User Registration, New User Registration Install).

Image: New User Registration Installation page 1 of 2

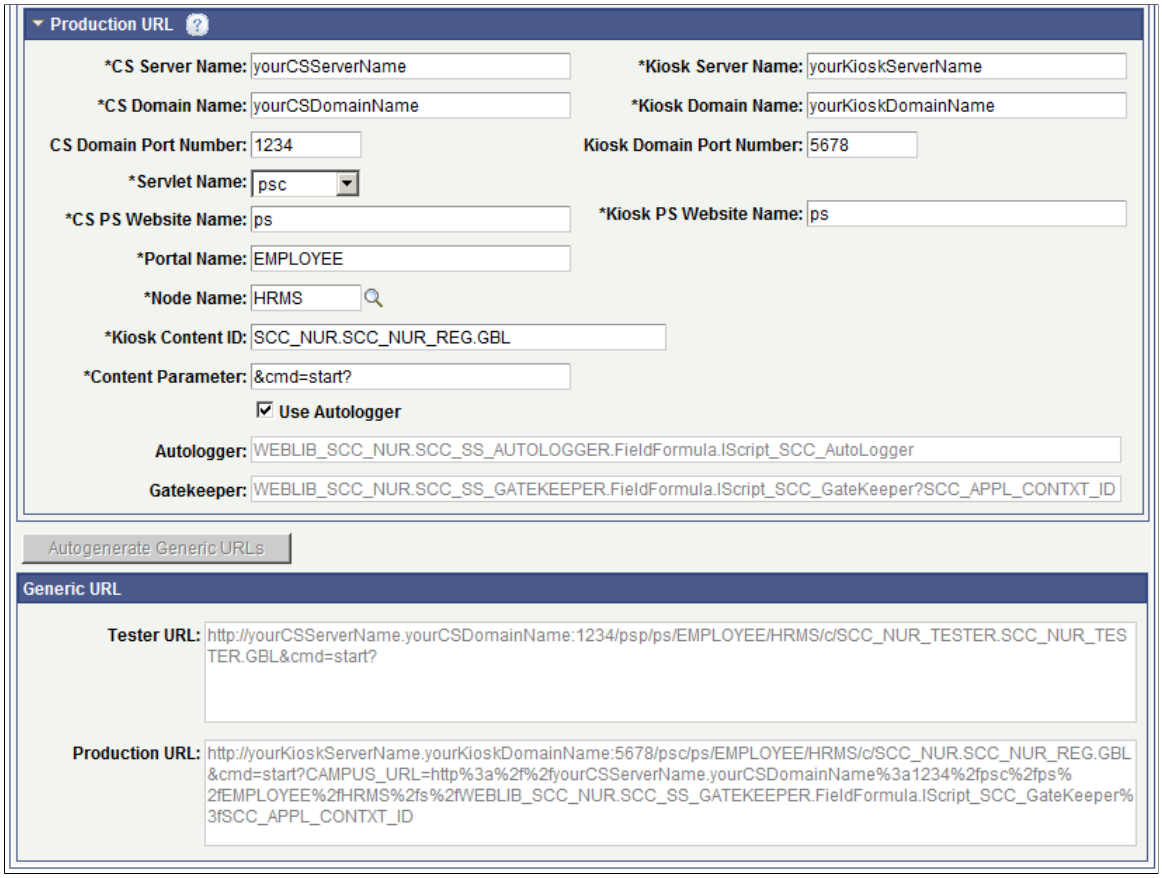
This example illustrates the fields and controls on the New User Registration Installation page 1 of 2. You can find definitions for the fields and controls later on this page.



 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Image: New User Registration Installation page 2 of 2

This example illustrates the fields and controls on the New User Registration Installation page 2 of 2. You can find definitions for the fields and controls later on this page.



The New User Registration Installation page lets you define the install options that are required for New User Registration.

Required values when creating an account

Select the field you want to define as a required field in a New User Registration service operation.

Email Address

By default, this check box is deselected.

Select this option if you want to require an email address to be entered when a user ID is created through the SCC_USERREG_CREATEACCT service operation. For example, when a user ID is created in the New User Registration sample login page or in the New User Registration Tester page. When you set the email address as a required field, users must enter an email address at account creation time.

Note: The email address entered at account creation time is used to populate the email address field in the newly created user profile. If you deploy the Forgot Password or Forgot User ID utility, an email address must exist in the user's profile.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Construct Generic URL to access NUR Logon Page

This group box contains information such as communication protocol and NUR constants (your environment parameters) that are necessary so the system can automatically generate a generic URL. The generic URL can be used to access the NUR sample login page or a custom version of it (production URL), or the NUR Tester page (tester URL) or both. The generic URLs, if a default NUR Context ID does not exist in your system, transfer the end user to the proper login page. Once the user is successfully authenticated, the user is transferred to the application home page. A specific application role level security is *not* provisioned and a transfer to an application-specific target page does not occur.

Communication Protocol

Specify the communication protocol prefix for the generic URL. By default, *https://* is selected. HTTPS ensures that the information that is transmitted over the network is secured through SSL/TLS.

New User Registration Constants

Use this group box to define the NUR constants that are needed to generate the Production and the Tester URLs.

Define Constants For

Select:

- *None.* By default, this value is selected. Use this value when you do not want to define any URL.

  If you select this value, the Production and Tester URL group boxes are disabled.

- *Both Production & Tester URLs* to specify the NUR constants for generating both the production and tester URLs.

  If you select this value, the Production and Tester URL group boxes are enabled.

- *Production URL* to specify the NUR constants for generating the production URL to access the NUR login sample page.

  If you select this value, the Production URL group box is enabled, and the Tester URL group box is disabled.

- *Tester URL* to specify the NUR constants for generating the tester URL to access the NUR Tester page.

  If you select this value, the Tester URL group box is enabled, and the Production URL group box is disabled.

Tester URL

Use this group box to specify the NUR constants that are required to construct the URL that transfers a user to the NUR Tester page.

CS Server Name

Enter the server name of the Campus Solutions database.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

CS Domain Name	Enter the domain name of the Campus Solutions database.
CS Domain Port Number	Enter the port number that your Campus Solutions database domain uses.
Servlet Name	Define the type of content that is used to build URLs. By default, no value is selected. Select: • psp for portal service type. If you select *psp* and populate the Tester URL group box, the URL that is created transfers the user to the NUR Tester page and shows the left menu navigation. This is okay because the Tester URL is used for testing purposes. • psc for content servlet type. If you select *psc* and populate the Production URL group box, the URL that is created transfers the user to the NUR login sample page (or your custom version of the page) and hides the left menu navigation.
CS PS Website Name (Campus Solutions PeopleSoft Website Name)	Enter the name of the website that was used when PeopleSoft Internet Architecture (PIA) was installed to create your Campus Solutions database. If you selected the default values when you installed the database, then you must enter *ps*.
Portal Name	Enter the name of the portal that is used to access the login page.
Node Name	Enter the name of the node that is used to access the login page.
NUR Tester Content ID	Enter the location of the NUR Tester page. The page is located in SCC_NUR_TESTER.SCC_NUR_TESTER.GBL. If you haven't changed the location, enter SCC_NUR_TESTER. SCC_NUR_TESTER.GBL. Otherwise, enter the information by concatenating its menu name, component name and market.
Content Parameter	Enter the query string parameter (name value pair) for the content. If you use PeopleTools as delivered, this value is "&cmd=start?" (without the quotes). This takes the user to the target page setup in the NUR Context ID mentioned in the URL.

Production URL

Use this group box to specify the NUR constants that are required to construct the URL that transfers a user to the NUR sample login page.

The fields in this group box are the same as the Tester URL, except for:

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Kiosk Server Name	Enter the server name of the environment where your kiosk is deployed.
Kiosk Domain Name	Enter the domain name of the environment where your kiosk is deployed.
Kiosk Domain Port Number	Enter the port number that your kiosk database domain uses.
Kiosk PS Website Name (Kiosk PeopleSoft Website Name)	Enter the name of the website that was used when PeopleSoft Pure Internet Architecture (PIA) was installed to create your kiosk database. If you selected the default values when you installed the database, then you must enter *ps*.
Kiosk Content ID	Enter the location of the NUR sample login page (or your own custom version of it). The page is located in SCC_NUR.SCC_NUR_REG.GBL. If you haven't changed the location, enter *SCC_NUR.SCC_NUR_REG.GBL*. Otherwise, enter the information by concatenating its menu name, component name and market.
Use Autologger	By default, this check box is selected. If you deselect this check box, the Autologger field does not appear. The Gatekeeper uses this check box to decide whether to allow users to be automatically logged in to your production page when they log in through your Kiosk, or to request users to enter their login credentials before they access your production page.
Autologger	This field does not appear if the Use Autologger check box is deselected. Otherwise, this field is view-only and displays the location of the Autologger that is used for NUR.
Gatekeeper	This field is view-only. It displays the location of the Gatekeeper that is used for New User Registration.
Sign In Command	This field is displayed when the Use Autologger is deselected. If the delivered Autologger logic is not used, enter the interface details where your transfer logic is stored.

Autogenerate Generic URL

Click to create the URL for either the production or tester URLs, or both. The generated URLs appear in the appropriate URL field.

This button is enabled only when you specify values for the NUR constants or change the communication protocol and then save the page.

Note: After you save the page, you must click the Autogenerate Generic URLs button in order to populate the Tester URL and the Production URL. If you close the page without auto-generating URLs, your self-service users are unable to access your login page through a URL.

 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Generic URL

This group box contains the generic production and tester URLs based on the installation options you specified. The generic URLs are later used to construct the specific URLs when you set up a NUR context ID for a specific online transaction. If an online transaction does not need to use a NUR context ID, you can give your users the generic URL to transfer them to your regular homepage. In this case, roles are not provisioned or page transfers do not occur.

Tester URL

This field is view-only. It displays the URL that your administrators can use to access the NUR Tester page. The tester page is used when you do not set up a kiosk, but want to test the URL with the tester page before you switch to production.

The NUR Tester page can also be accessed by your administrators by navigating to Setup SACR, System Administration, Utilities, Sample User Interfaces, New User Registration Tester. Use the Tester URL to test your NUR Constants values and the NUR Context ID settings that are needed for a specific online transaction.

Production URL

This field is view-only. It displays the URL that your users can use to access the NUR login sample page or your custom version of the sample login page. The NUR login sample page is used when you set up a kiosk.

When you deploy a kiosk database, make sure the values you specify in the New User Registration Installation page are the same you enter in your production database.

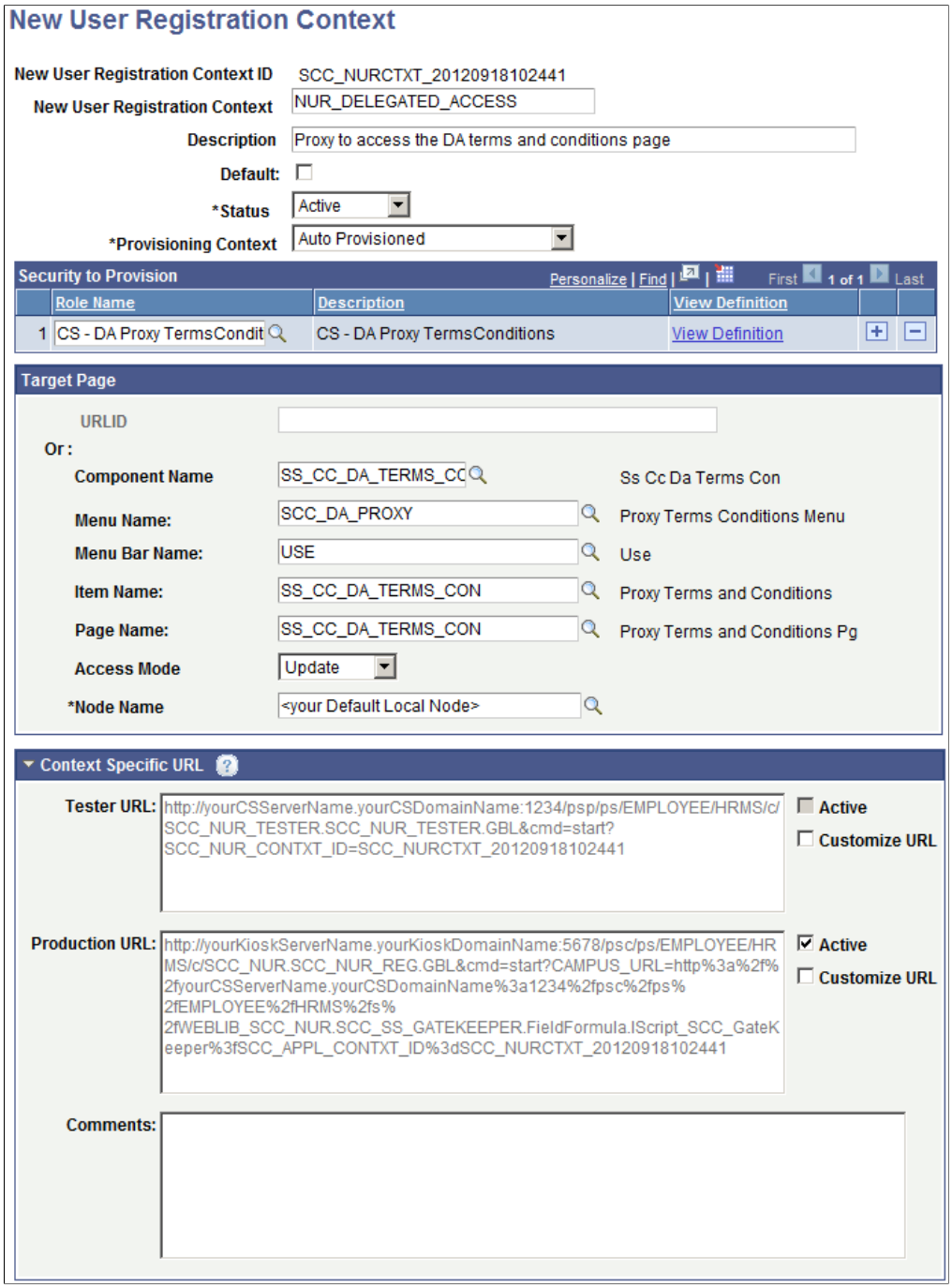
Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Setting Up New User Registration Context

Access the New User Registration Context page (Set Up SACR, System Administration, Utilities, New User Registration, New User Registration Context).

Image: New User Registration Context page

This example illustrates the fields and controls on the New User Registration Context page. You can find definitions for the fields and controls later on this page.



Create a NUR context ID only if the online self-service transaction requires the user to be either provisioned with application-specific security roles or needs to be transferred to a specific target page.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The NUR context ID is used by the NUR framework only when it is embedded in the URL you provide to your users to access your login page.

By default, once the New User Registration Installation page is populated the URL is automatically created for you. While you can directly provide the URL to your users, we recommend to programmatically retrieving the URL by evaluating which one is marked as Active.

New User Registration Context ID

Displays the unique ID that the system assigns when you add a NUR context.

When you add a context, this field displays the value NOID until you save the record. When you save the new context, the field displays the ID that the system assigned to the context.

By default, the context ID is automatically appended to the generic URLs you auto-generated in the NUR Installation page. The resulting URLs are then specific to the online self-service transaction. The NUR framework uses this value, which is embedded in the URL used to log in to your system, to assign the security roles and/or transfer the user to the target page accordingly.

New User Registration Context

Enter the name of the context for the NUR context ID. For example, if you create a NUR context ID so users can access your Admissions online application page, you could enter *Online Application*.

Description

Enter a longer description for the New User Registration context (50 characters).

Default

Select to mark the NUR context as default. Only one NUR context can be marked as default.

The system uses the default NUR context when a NUR context is not passed in the URL that the user clicks to access the login page. When the NUR context is not passed, the system looks for the default NUR context ID.

If the system does not find the default context ID or the default context ID is inactive, then the user is transferred to the home page and application-specific security roles are not provisioned.

Note: It is optional to pass the NUR context in the URL.

Status

Select to set status. Default is *Active.*

If the URL provided to your users to access your system refers to an inactive NUR context, then the URL is embedded with “No URL defined.” Your users are unable to access your login page.

Provisioning Context

Select *Auto Provisioned* if context should be Public.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

When Auto Provisioned is selected, the guest or the returning user is provisioned with application role level security dynamically just-in-time by the Gatekeeper. The Gatekeeper gets these roles from the list of roles you select in the Security to Provision grid. After real-time provisioning, the user is redirected to the specified target page, if one is provided.

(Optional) Security to Provision

Use this grid to define a list of security roles that are specific to the consuming self-service transaction (such as AAWS Online Application or Delegated Access) for which the New User Registration context is created. The roles that you enter in this grid are assigned only to the users who are successfully authenticated by the NUR framework for a specific consuming self-service transaction. These roles are assigned by the Gatekeeper to the user profile of the newly created user or the returning user after the user is successfully authenticated by your system.

Role Name

Select the application-level security role names that you want to provision the user's profile going through the NUR framework with this NUR context. The prompt returns the roles set up in the PeopleTools Roles component (PeopleTools, Security, Permissions & Roles, Roles).

If you specify a target page, make sure you enter a role name that grants access to the specified target page. Otherwise, the user is not transferred to the target page due to lack of security.

(Optional) Target Page

Depending on the online self-service transaction that consumes NUR, it may make sense to transfer the user directly to a target page instead of making the user manually navigate to the desired page after successful authentication into the system. For instance, if you have deployed an online application self-service transaction, the system can direct the user to your Online Application homepage. In Delegated Access, the system should direct the proxy directly to the very first page that the proxy should access to take advantage of the delegated accesses (the Proxy Terms and Conditions page). The target page can also be an external URL.

If you do not identify the target page in this group box, the user is redirected to the application home page.

URL

If the target page lies outside the PeopleSoft system, provide the URL to access the page. After successful authentication, the user is immediately transferred to the URL address.

Component Name, **Menu Name**, **Bar Name**, **Item Name**, **Page Name**

If the target page is built within the PeopleSoft system, list the menu objects to retrieve the proper page.

If you are using an external UI that lies outside the PeopleSoft system (a URL ID), these fields are disabled.

Access Mode

Select the mode in which the target page, built within the PeopleSoft system, should open when the user is transferred to

 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

the target page. Applicable values are: Add, Correction, Update and Update All.

See Access Mode field.

Node Name

This is a required field regardless of whether the target page is a URL or a PeopleSoft component name.

Select the name of the local node defined for the database where the target page is located (for a typical installation, select your default local node). The default local node is defined in the Integration Broker Nodes component (PeopleTools, Integration Broker, Integration Setup, Nodes). The Gatekeeper uses this node to transfer the user to the specified target page.

Your system includes the following NUR context IDs:

- SCC_NURCTXT_20120918102441 - NUR_DELEGATED _ACCESS (used for Delegated Access functionality)
- SCC_NURCTXT_20130211110717 - NUR_CHANGE_ PASSWORD (used by the NUR Forgot Password utility)

If you intend to use these contexts, you must update the Node Name from the default value ‘LOCAL’ to your local node name.

Access Mode field

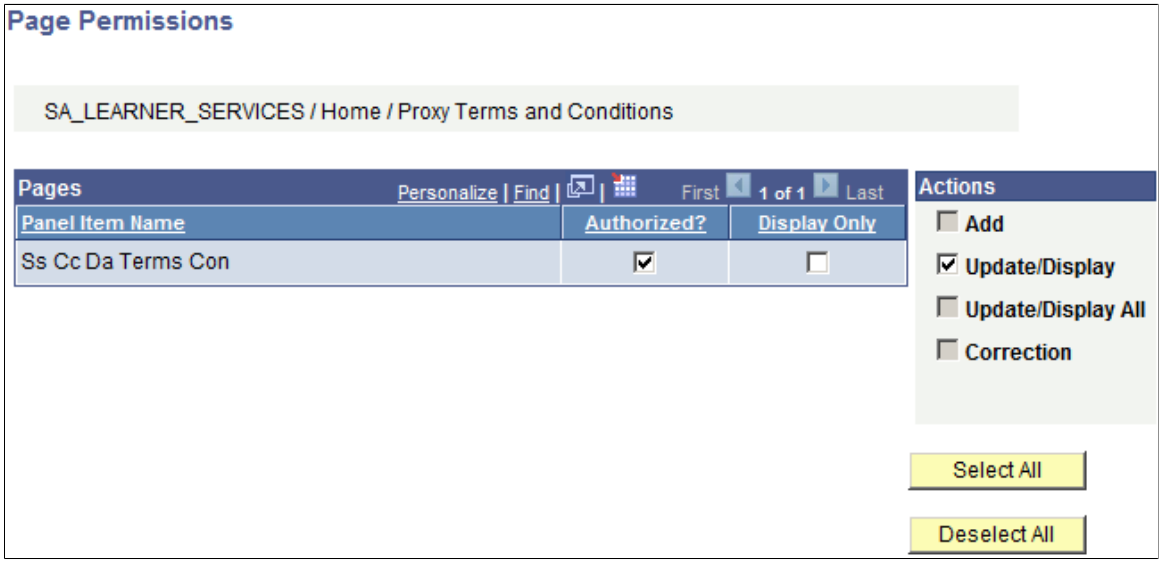
If one of the roles you list in the Security to Provision grid includes a permission list that grants access to the component and menu names that are listed in the Target Page group box, make sure you select the action mode used in the permission list for the page name you select. For example, the image that illustrates the NUR Context page shows the role ‘CS - DA Proxy TermsConditions’. This role contains a permission list that grants access to the SCC_DA_PROXY menu and the SS_CC_DA_TERMS_CON

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

component, which contains the page SS_CC_DA_TERMS_CON. When you open the page permission, the Actions selected is Update/Display. You should select Update.

Image: Page Permissions page

This example illustrates the fields and controls on the Page Permissions page..



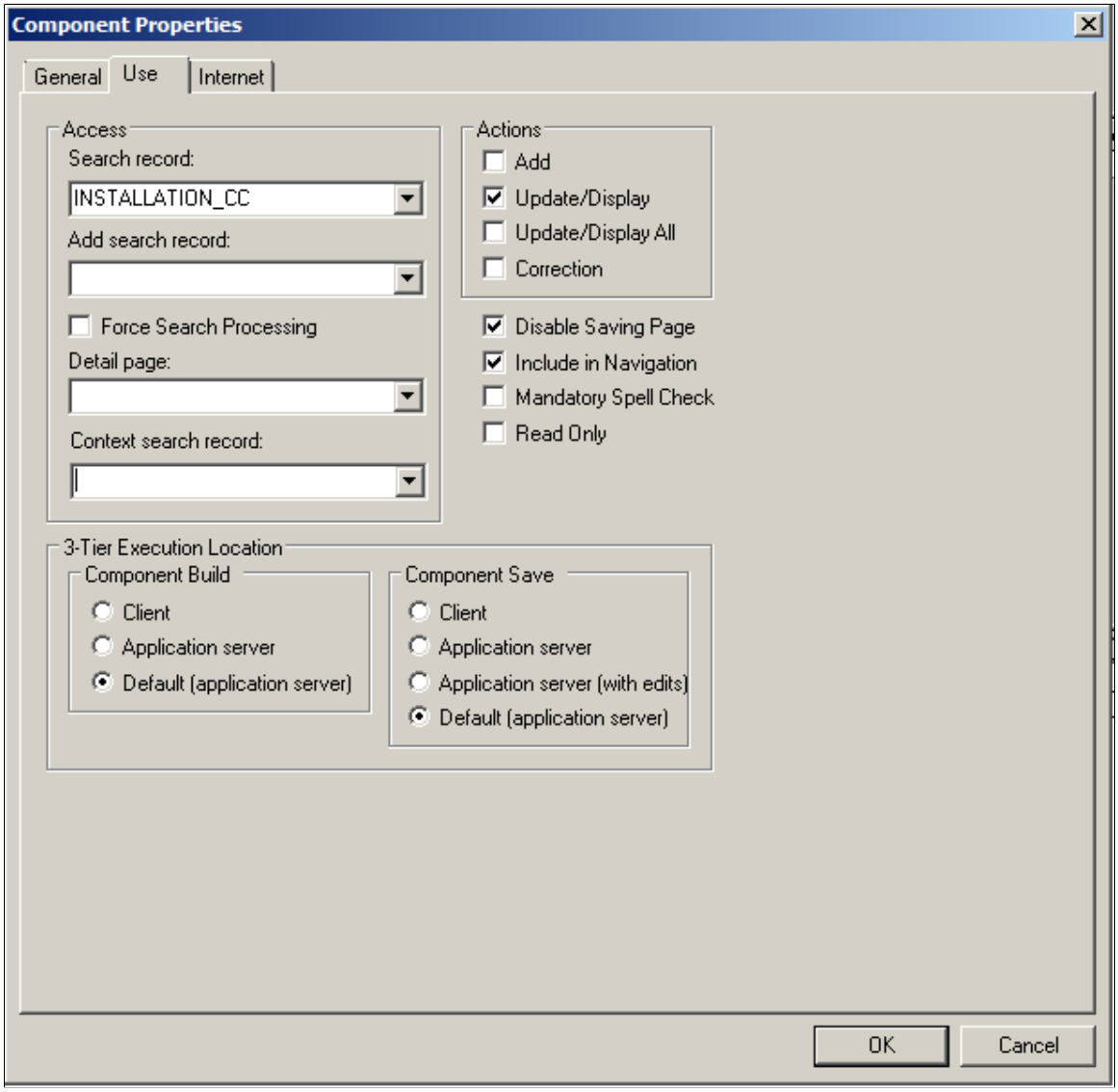
If you did not list any roles, make sure you select an Action Mode for which the component was created. For example, the preceding graphic shows the component name SS_CC_DA_TERMS_CON. If you open

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

this component using Application Designer, the Component Properties show that the possible Actions selected is Update/Display. In this case, you select Update.

Image: Component Properties window

This example illustrates the fields and controls on the Component Properties window.



Context Specific URL

By default, the URLs that appear in this group box are the respective auto-generated URLs from the New User Registration Installation page appended with the NUR context ID that is specific to the NUR consumer. The Tester URL transfers the proxy to the NUR Tester login page and the Production URL transfers the user to the NUR sample login page or your own custom version of the page.

If you did not auto-generate the generic URL for any one of these fields, then these fields do not display any value.

If you select the corresponding Customize URL for any one of these fields, the field becomes editable and you can specify your own URL. For example, in the Production URL field you can specify the URL to your custom login page. You can specify your own URL even if you do not use the NUR framework.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The Active checkbox allows you to test the deployment of your online self-service transaction by selecting the Tester URL. When your self-service transaction is ready, make sure you set the Production URL to Active. The Active checkbox allows you to test a new online self-service transaction while others may be in production.

The specific Production and Tester URL can be directly provided to your users to access (or test) your login page and do the proper authentication. However, it is recommended to programmatically retrieve the URL that is marked as Active. This way you will always be certain the URL is updated with the latest installation information. For example, if your Campus Solutions domain port number is modified in the New User Registration Installation page, the new port number will be automatically reflected in the specific URL.

By default, the Active and Customize URL check boxes for the Production and Tester URLs are deselected.

Only one URL can be active at any one time. Use the Tester URL only for testing the deployment of your online self-service transaction. When your self-service transaction is ready, make sure you come back to the NUR context ID settings to set the Production URL to Active.

Production URL

Displays the URL that is used to access the NUR sample login page or your custom version of the page.

The production URL is used when you set up a kiosk for the production environment.

If you select the:

- Active check box for the Production URL, then the Active check box for the Tester URL is disabled.
- Customize URL check box for the Production URL, then the production URL can be edited; you can enter the URL of your choice.

Tester URL

Displays the URL that is used to access the NUR Tester page.

The tester URL is used when you do not set up a kiosk, but want to test the URL with the NUR Tester page before you switch to production.

If you select the:

- Active check box for the Tester URL, then the Active check box for the Production URL is disabled.
- Customize URL check box for the Tester URL, then the tester URL can be edited; you can enter the URL of your choice.

Related Links

Step 7: Creating a URL to Access the New User Registration Login page

 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Provisioning Access Through the Gatekeeper

The Gatekeeper is a Campus Solutions security utility that has the responsibility of dynamically provisioning application level security access and navigational orchestration to Campus Solutions pages or even navigation outside of Campus Solutions to a newly authenticated user. Prior to redirecting a user to a specific target page, the Gatekeeper is also responsible for validating that the self-service requestor is authorized (provisioned) to access a particular self-service application.

The New User Registration framework is PeopleTools web service based and therefore usable from any technology that supports SOAP over HTTP web service integration.

The Gatekeeper and New User Registration

The New User Registration framework, after having successfully authenticated a user to your system, uses the Gatekeeper to optionally perform the following two tasks:

1. Provisions the newly authenticated user with the security needed to perform the self-service transaction for which the user has signed in through New User Registration.
2. Transfers the newly authenticated user to the target page defined for the self-service transaction for which the user has signed in through New User Registration.

The application level provisioning is performed just-in-time. The user's user profile is being provisioned with the roles listed in the New User Registration Context ID used at the final moment when the user accesses the Campus system to perform a specific self-service transaction. Once provisioning is completed, if a target page is entered in the New User Registration Context ID, the Gatekeeper verifies the user has security access to the target page and if so, transfers the user.

The context in which the security role and the target page are defined is specific to the self-service transaction. The information is set up in the New User Registration Context setup page and stored under a New User Registration Context ID. The New User Registration Context ID is what the Gatekeeper needs to know to perform the security provisioning and the page transfer.

The use of the Gatekeeper within New User Registration is possible when the New User Registration login page is accessed from a launching point to perform a subsequent self-service transaction. For example, from your institution's web site, you could advertise that it is possible to apply online at your institution and display a Click here to apply link. The link URL must include:

- the content reference where the New User Registration login page is located so the user can be redirected to it
- gatekeeper information
- (optional) New User Registration context ID

From the launching point, the user is transferred to the New User Registration login page. Once successfully authenticated, New User Registration, through the Gatekeeper and the New User Registration Context ID passed in the URL, provisions the security role(s) related to the self-service transaction (for example, security role needed to access the Online Application page) and then transfers the user directly to the target page defined for performing the self-service transaction for which the user launched the New User Registration process. When no New User Registration Context ID is passed, the Gatekeeper uses the New User Registration Context ID you marked as the default.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Warning! When you deploy New User Registration framework, all the existing users you have in your system need to have access to the Gatekeeper in order to use their existing user ID to sign in through a New User Registration login page. The new users (the guest creating a user ID through New User Registration) are provisioned with the Gatekeeper security as part of the "basic provisioning" defined in the SCC_SS_TEMPLATE user ID.

Related Links

Setting Up New User Registration Context

Step 1: Initial Setup for New User Registration

Step 7: Creating a URL to Access the New User Registration Login page

Step 8: Provisioning the Gatekeeper Permission List to all of Your Users

Deploying New User Registration

This section presents some examples for deploying New User Registration. Institutions can adopt these examples, only pieces of it, or continue using their own security implementation (for example, with an identity management solution, LDAP or any other user management system).

The New User Registration login page should be accessed from where an unidentified user wants to perform a specific transaction that requires signing in to your system.

New User Registration can be triggered from a:

- Launching object on the institution's web site. For example, a link, a button, or an image.
- URL sent through an email notification.

For example, if you deployed an Online Application self-service transaction, your portal may include a button or a link "Click here to apply online." The URL you configure behind the button or the link can contain information to first transfer the future applicant to the New User Registration login page (or your custom version of it) prior to being transferred directly to your online application page. For these events to occur, the URL must contain information about which context the self-service transaction is performed. Another example for accessing the New User Registration login page is when a user receives an email notification and you include a link in the text so the user can easily sign in to your system and perform a specific transaction. Your system comes with the Delegated Access functionality that uses this deployment: proxies receive an email notification that instructs them how to access the system (includes a hyperlink), accept the terms and conditions, and review the access delegated by a specific person.

The underlying steps involved in providing an anonymous user access to your Campus Solutions system to perform a specific online transaction are as follows:

1. Use the New User Registration Installation page to generate the generic URL that you embed in the link, button, UI element, or email message. Optionally, if the online self-service transaction requires provisioning the newly authenticated user with application-specific security role or needs to transfer that same user to a specific target page, use the New User Registration Context page to automatically create a URL specific to that transaction.
2. Have your guests or returning users access the New User Registration login page by either:

 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

- Sending them an email notification that contains the link to access your Campus Solutions system. The link is a URL that transfers users to your NUR login page.
- Providing a button, link, or any other UI element in your portal or web site to invite users to perform a self-service transaction. The UI element is embedded with a URL that redirects users to your NUR login page. You can place the UI element on a website outside of your Campus Solutions system.

3. If users already have an account, they can use their existing account to sign in to your system. The authentication occurs through the NUR authenticate service operation, vanilla PeopleTools login page, or a federated login page.
4. If users do not have an account, they can register a new account through the NUR login page. The user profile creation occurs through the NUR Create Account service operation. The NUR authenticate service operation authenticates users and, if authentication is successful, allows them to sign in.
5. After a user is authenticated, the Gatekeeper interrogates the URL queryString parameter to determine which context (NUR context ID) the user requests access to. The Gatekeeper uses the user ID (OPRID) and a combination of the SCC_IDM_PROVISN and SCC_IDM_APPS tables to determine whether the user has been given access to the application or needs to be given just-in-time access.

   SCC_IDM_APPS contains the setup for the specific NUR context ID, or the setup for the NUR Context ID that is marked as default.

   SCC_IDM_PROVISN contains all the user profiles that have been previously provisioned a security role from a specific NUR Context ID.
6. If a NUR context ID is found and it contains a security role that must be provisioned, the system calls the Campus Identity Manager provisionTran() API method. This method provisions the user profile with the roles contained in the NUR context ID in real time.
7. If the NUR context ID also contains a target page, the Gatekeeper validates whether the user has the required security to access the target page. If so, the Gatekeeper transfers the user to the target page. Otherwise, an error appears and the user is not transferred.

Note: The New User Registration framework uses the PeopleTools security validation and authentication logic.

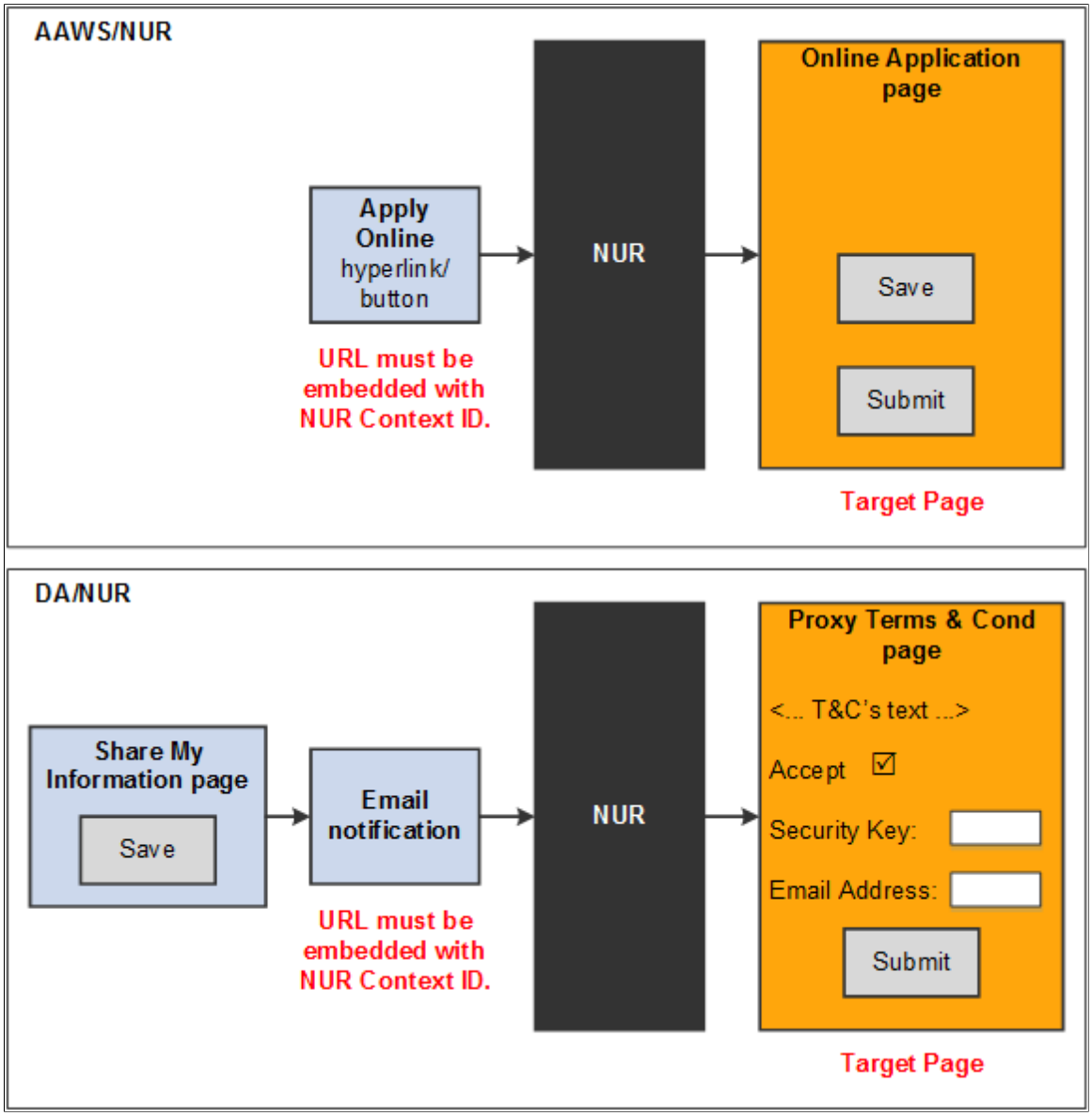
The following diagram illustrates where New User Registration (NUR) takes place when it is triggered from a button, link, or any other UI element located outside of your Campus Solutions system, for

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

example, as part of your Online Application (AAWS) transaction; and when it is triggered from a link (a URL) in an email notification, for example as part of the Delegated Access (DA) process:

Image: Example of a Self-Service Transaction using New User Registration

Example of a Self-Service Transaction using New User Registration



The diagram shows that NUR is considered a black box, independent from any logic specific to the online self-service transactions that are consuming it. New User Registration takes place before performing the self-service transaction. This is because within PeopleTools security management the security must be provisioned before a component is accessed.

The following describes the logic in the New User Registration black block.

1. Users click a link or button or any other user interface elements configured with a URL that is embedded with a NUR context ID (this link could be on the institution's website or in an email message).

 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

2. The login page authenticates the user (and provides the option of creating a user account). An institution can implement this through the NUR service operations. After successful authentication or account creation, the gatekeeper provisions security defined in the NUR context ID that is passed, then redirects the user to the target page to perform the self-service transaction.

3. The user registration page should be publicly accessible to anonymous users.

4. 4. The New User Registration web service operations inspect the SCC_IDM_PROVISN record to determine which applications the user has access to. The information is then returned to the user interface in the web service operation response message. The user interface may choose to use this information to assist in the user navigation. The <URL> attribute contains the link to access the target page specified for the NUR Context ID in the NUR Context setup page. For example, the following Create Account or Authentication service operation response message shows that the newly authenticated user should be transferred to the SS_CC_DA_TERMS_CON page, which is the target page for the Delegated Access application:

```
<NUR_REGISTRATION_CONTEXT>
 <SCC_APPL_CONTXT_ID>SCC_NURCTXT_20120918102441</SCC_APPL_CONTXT_ID>
 <SCC_APPL_CONTEXT>NUR_DELEGATED_ACCESS</SCC_APPL_CONTEXT>
 <URL>https://yourCSServerName.yourCSDomainName:1234/psc/ps/EMPLOYEE/HRMS/C/SC⇒
C_DA_PROXY.SS_CC_DA_TERMS_CON.GBL&amp;cmd=start?</URL>
</NUR_REGISTRATION_CONTEXT>
```

If you do use the NUR framework as it is delivered, you do not need to configure you user interface to read the response message in order to transfer your user to the proper target page. The Gatekeeper does it for you.

Note: The <URL> attribute is populated with the link to access the target page defined for the returned NUR Context ID. If the target page was defined as an external URL (a URLID was populated), the same value is populated between the tags. If the target page was defined as a PeopleSoft Architecture (PIA) page, then the link is constructed using the New User Registration Installation values entered for the Production URL and embedded with the specified target page.

---

5. If you do not use the NUR context and want to implement real-time application processing, then you must include the logic in your applications to call the Campus Identity Manager IDM interface method API, provisionApp(), to insert a row to the provisioning table, SCC_IDM_PROVISN. This could be done, for example, from an online component.

6. When a user is successfully authenticated, the URL that contains the context is processed. The Gatekeeper checks the provisioning context defined in the NUR context ID. These are the possible outcomes:

   - A NUR context ID does not exist. If this is the case, the Gatekeeper responds with an error that is equivalent to an HTTP 403 Forbidden response - Failed attempt.

   - A NUR Context ID exists with a target page defined, but the user does not have security access to the target page. In this case, the Gatekeeper responds with an error that is equivalent to an HTTP 401 Unauthorized response - Failed attempt.

   - A NUR Context ID exists with a target page defined and the user has security access to the target page. The Gatekeeper performs a lookup on the NURContext configuration table based on the supplied SCC_APPL_CONTEXT and responds with an HTTP redirect that is equivalent to a 407 Temporary redirect response - Successful attempt.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

7. At this point, control falls within the domain of the individual application.

   If an application requires further real-time transaction-level provisioning, then you must include a logic in the application to call the Campus Identity Manager IDM interface method (API, provisionTran(), to insert a row in the SCC_IDM_PROVISN provisioning table. This could be done, for example, from an online component.

Developer Reference to Deploy New User Registration

Bundle 45: PeopleTools is introducing changes in the Distributed User Profile functionality effective with release 8.54.26. These changes impact New User Registration security objects. This PeopleTools release will mandate:

1. the use of new Component Interfaces (CIs):
   a. USERPROFDIST_ADD_CI
   b. USERPROFDIST_UPD_CI
   c. USERPROFDIST_ADM_CI
2. the use of Remote Security Administrator Role Grant Capability in order to provision roles to other users.

Campus Solutions customers who deploy New User Registration (NUR) will want to assess their security setup for roles and permission which interact with the NUR Gatekeeper and modify as noted in the table in Step 1 > Creating a Role.

Step 1: Initial Setup for New User Registration

To create user accounts, New User Registration requires two pre-defined user profiles set with the following user IDs: SCC_GUEST and SCC_SS_TEMPLATE.

Once created, those user profiles can be used as templates to grant your guests basic security access to your PeopleSoft system.

To be provisioned with application level security and transfer to a specific target page, the newly created user ID must be provisioned with a security role granting access to the Gatekeeper.

Creating a Role

You must create a role that contains security access to the security objects that is needed to use New User Registration (e.g. Gatekeeper and Forgot Password/Forgot User ID utilities). To create the role, use the Roles component (PeopleTools, Security, Permissions & Roles, Roles), then enter the following information:

Field	***Value***
Role Name	<name of your choice. E.g.’CS - NUR GateKeeper’>

 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Field	***Value***
Description	<description of your choice>

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Field	***Value***

Permission Lists	HCCPCSSA1200 - CS NUR GateKeeper. This permission list is delivered with your system. It grants security access to generic NUR objects:
	• Web library: WEBLIB_SCC_NUR. This web library contains the following permissions and access should be set accordingly:
	  • SCC_SS_AUTOLOGGER.FieldFormula.IScript_SCC_AutoLogger = Full Access
	  • SCC_SS_GATEKEEPER.FieldFormula.IScript_SCC_GateKeeper = Full Access
	  • SCC_SS_GATEKEEPER.FieldFormula.IScript_SCC_setPSToken The function is set with Access Permissions = No Access.
	• Page access
	  • Menu Name = SCC_NUR
	  • Component Name = SCC_NUR_REG (contains the delivered sample NUR Sample login page)
	• Web services used for generic registration and authentication logic
	  • SCC_USERREG_AUTHENTICATION (Full Access)
	  • SCC_USERREG_CREATEACCT (Full Access)
	Bundle 45: HCCPCSSA1210 - CS NUR Utilities is a delivered Permission List. It has been re-delivered to include new Component Interfaces (CIs) on the Component Interface tab.
	HCCPCSSA1210 - CS NUR Utilities. This permission list is delivered with your system. It grants security access to optional NUR utilities such as Forgot Password and Forgot User ID:
	• Page access to the PeopleTools delivered ‘Change My Password’
	  • Menu Name = MAINTAIN_SECURITY
	  • Component Name = CHANGE_PASSWORD

 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Field	*Value*

	• Web services used for the Forgot Password and the Forgot User ID utilities:
	  • SCC_USERREG_GET_PASSWORD (Full Access)
	  • SCC_USERREG_GET_USERID (Full Access)
	  • SCC_USERREG_GET_PSWD_HINT (Full Access)
	• Component Interface: SCC_NUR_EMAIL_PSWD
	  • Cancel – Full Access
	  • Find – Full Access
	  • Get – Full Access
	  • Save – Full Access
	• Component Interface: USERPROFDIST_ADD_CI
	  • Cancel – Full Access
	  • Find – Full Access
	  • Get – Full Access
	  • Save – Full Access
	• Component Interface: USERPROFDIST_UPD_CI
	  • Cancel – Full Access
	  • Find – Full Access
	  • Get – Full Access
	  • Save – Full Access
	• Allow Password to be Emailed = ‘Y’ (used for the Forgot Password utility).

Bundle 45: Added row. Role Grant	Any role which includes permission lists which allow NUR Gatekeeper access and is used to grant security access to other roles must include Role Grant definitions.

Bundle 45: Added cross-reference.

See *PeopleTools: Security Administration*, “Implementing Distributed User Profiles”.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Creating SCC_GUEST user ID

In PeopleTools 8.5+, any anonymous inbound request originates from the ANONYMOUS node. For example, when a guest (unknown person) requests for a user ID, the user registration service operation associates the request with the ANONYMOUS node.

To enable anonymous access to Campus Solutions web services in a secure fashion, the PeopleSoft system, by default, associates all anonymous requests with a default account: SCC_GUEST. Therefore, to use New User Registration, you need to set up a default user profile that has minimal system access. This default user profile should be set with the User ID SCC_GUEST.

To create the SCC_GUEST account, use the User Profiles component (PeopleTools, Security, User Profiles, User Profiles) and enter the following information:

User ID	SCC_GUEST
Symbolic ID	<As defined for your institution>
Password	<password of your choice>
Confirm Password	<password of your choice>
Language Code	<Language of your choice>
ID Type	None
Role Name	PeopleTools and Standard Non-Page Permissions and either CS – NUR GateKeeper or the role name you created above to grant access to the New User Registration Gatekeeper. **Note:** The anonymous user needs access to a role that contains the permission list HCCPCSSA1210 – CS NUR Utilities. In this way, the anonymous user can use the Forgot User ID and Forgot Password utilities.

Perform the following steps to update the ANONYMOUS Integration Broker node:

1. Access the Node Definitions page (PeopleTools, Integration Broker, Integration Setup, Nodes), and select Node Name *ANONYMOUS*.
2. In the Node Definitions tab, ensure that Node Type is set to *External*, the Default User ID is set to *SCC_GUEST*, and the Active Node and Segment Aware options are selected.
3. In the WS Security tab, enable WS-Security for this node by selecting an authentication token type (for instance Username Token).

Note: It is assumed that you have performed and validated all the basic Integration Broker setups prior to setting up the node. See *PeopleTools: Integration Broker* for information on Integration Broker gateway setup and service configuration.

Creating SCC_SS_TEMPLATE User ID

After successfully processing the user registration request, the user registration service operation creates a new account for the user. In other words, the service operation creates a PeopleTools user profile for the

 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

guest. The service operation uses the template account SCC_SS_TEMPLATE to clone its security setup and create a new account for the guest.

Create the SCC_SS_TEMPLATE account and assign any common default values that your institution wants new users to automatically receive when registering. To be authenticated to your system through New User Registration, the new user needs to have access to the Gatekeeper. Add to this user ID template the role you created above to grant access to the Gatekeeper.

To create the SCC_SS_TEMPLATE account, use the User Profiles component (PeopleTools, Security, User Profiles, User Profiles) and enter the following information:

User ID	Enter *SCC_SS_TEMPLATE.*
Symbolic ID	<As defined for your institution>
Password	<password of your choice>
Confirm Password	<password of your choice>
Language Code	<Language of your choice>
Navigator Homepage	Enter *HCSPNAVHP.*
Process Profile	Enter *HCSPPRFL.*
Primary	Enter *HCPPALL.* Identifying a Primary Permission List is needed for personal data information getting its security information from there. For example, Citizenship, Visa Permit, Demographic Data Access (DDA), and so on.
Row Security	Enter *HCDPALL.*
ID Type	None
Role Name	Examples: PeopleSoft User, Standard Non-Page Permissions and either CS – NUR GateKeeper or the role name you created above to grant access to the New User Registration Gatekeeper. Also, add any other roles you want to grant access your guests at the moment of registering. Make sure the role names you include in this generic user ID template only grant access to basic components and security objects to access your PeopleSoft Campus Solutions system. The role names provided here are only examples.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Warning! The information given in the grid above related to SCC_SS_TEMPLATE role assignment and configuration are for use only in a testing or demo environment. Before migrating your transaction setup and the web services to a production environment, it is recommended that you complete a thorough analysis of your institution's security requirements.
It is also recommended that you allocate the SCC_SS_TEMPLATE user ID only a minimal amount of system access that is required to execute the needed web services for your self-service transactions. You define Web Services access under PeopleTools, Security, Permissions & Roles, Permission Lists, Web Services. For instance, any roles that you assign to the SCC_SS_TEMPLATE should contain at least a Permission List that has access to the following web services:

Web Services	***Service Operations***	***Access***	***Definition***
<custom services>	<custom service operations>	Full Access	Web services you created to perform your self-service transactions. For example, to perform the AAWS online application transactions, select Service *SAD_ADMISSIONS* and select Full Access to each of the service operations. If you setup a transaction for Delegated Access, select Service *SCC_DA* and select Full Access to each of the service operations.
SCC_USERREG	SCC_USERREG_ AUTHENTICATE SCC_USERREG_ CREATEACCT	Full Access	Web services to use New User Registration and User Authentication.
SCC_LOV	SCC_GET_LOV	Full Access	Optional. Web service to use List of Values.
SCC_SM_SERVICE	SCC_SM_SERVICE_SYNC	Full Access	Optional. Grant access only if you use External Search/ Match.
SCC_SM_FETCH	SCC_SM_FETCH_SYNC	Full Access	Optional. Grant access only if you use External Search/ Match.

Similarly, any roles that you assign to the SCC_SS_TEMPLATE user ID template should contain at least a Permission List that has access to the following HCM component interfaces that are required to operate these services (which are used by CTM to access the HCM Person data):

- HCR_EMPLOYEE_CHECKLIST_SRV
- HCR_IDENTIFICATN_DATA_SRV

 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

- HCR_JOB_DATA_POI_SRV
- HCR_MIL_EE_TRK_SRV
- HCR_NAMES_OTHER_SRV
- HCR_PERSONAL_DATA_SRV

Assigning Specific Security Roles to a User

Because different online transactions integrated with New User Registration can have their own security needs, each online transaction can define these roles in the New User Registration Context page.

See Step 3: Defining New User Registration Contexts.

Step 2: Validating the CTM Transaction Delivered for New User Registration

See Setting Up CTM for New User Registration.

(Optional) Step 3: Defining New User Registration Contexts

For each of the online transactions you want to integrate with New User Registration, create a New User Registration Context ID or create a New User Registration Context ID that serves as default.

See Setting Up New User Registration Context.

Step 4: Designing Your Registration or Login page

See Using the New User Registration Sample User Interfaces.

Step 5: Setting Up a Kiosk

Set up the following on the database of the Kiosk:

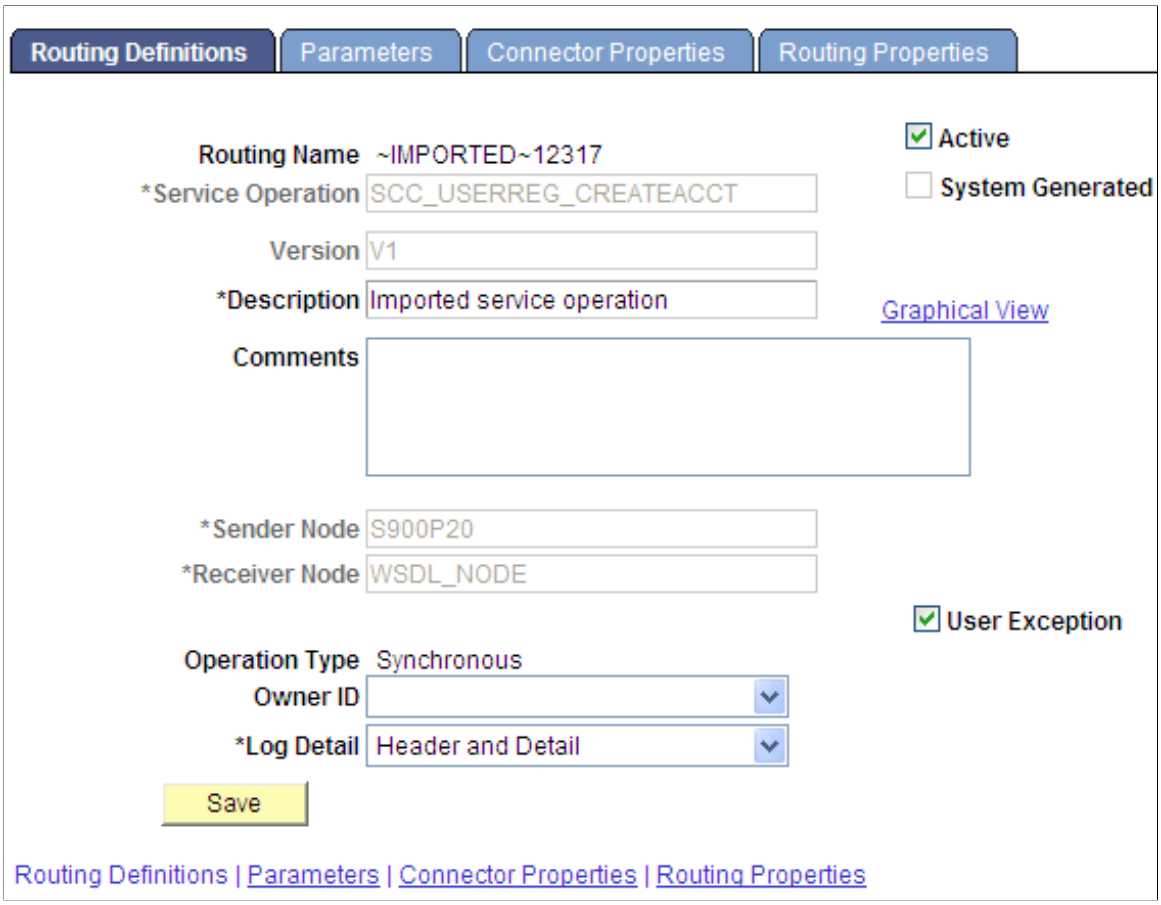
- The User Exception check box needs to set on the Routing Definition page of the Kiosk. When the check box is selected, in case an error is encountered during processing it allows the system to capture the SOAP fault and display it. Else, when the check box is not selected the system responds with a

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

HTTP 500 error. To access the Routing Definition page, select PeopleTools, Integration Broker, Integration Setup, Routings.

Image: Routing Definitions page

This example illustrates the fields and controls on the Routing Definitions page. You can find definitions for the fields and controls later on this page.

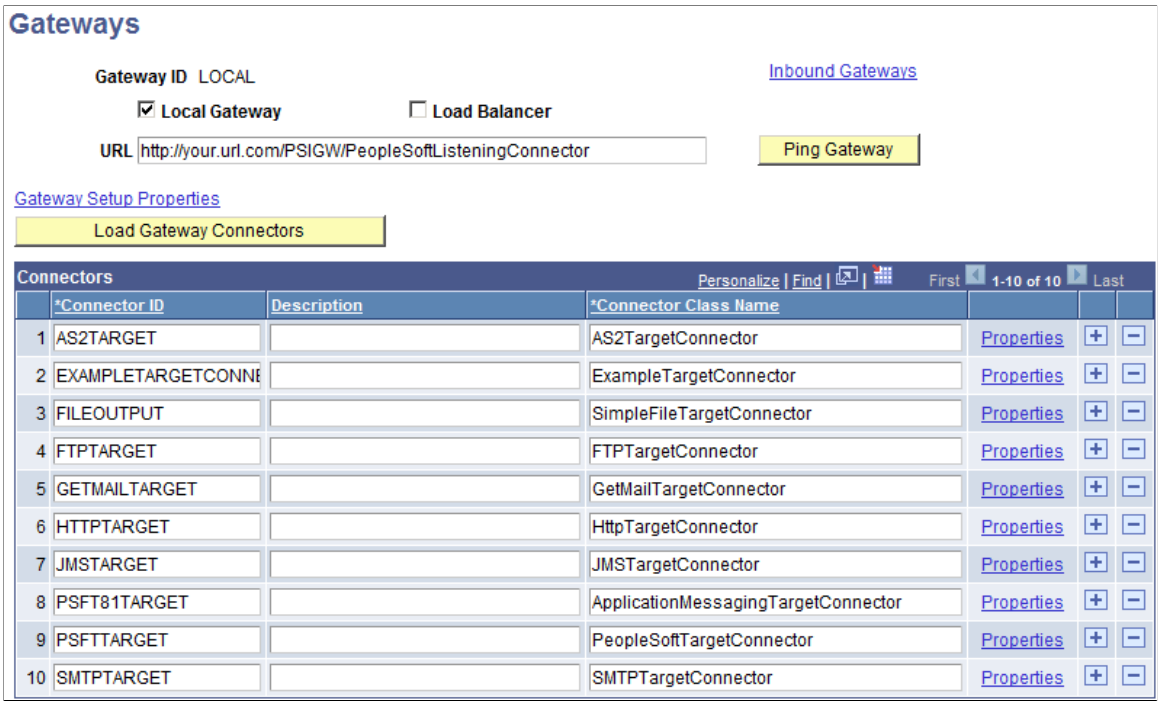


 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

- Verify that the gateway is active. To access the Gateways page, select PeopleTools, Integration Broker, Configuration, Gateways.

  Image: Gateways page

  This example illustrates the fields and controls on the Gateways page. You can find definitions for the fields and controls later on this page.



Press the Ping Gateway button to make sure the gateway is active. The Status displays ACTIVE.

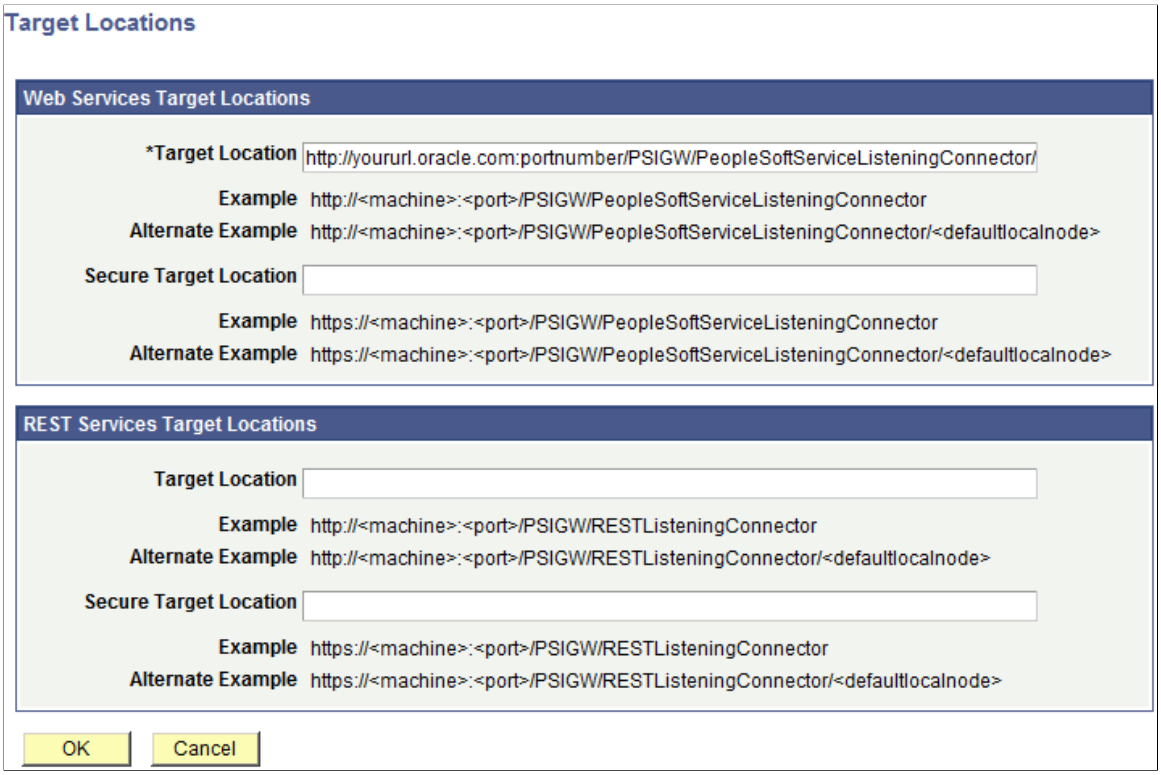
Note: The gateway needs to be active on both the Kiosk as well as the production environments.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

- Verify that the setup target location is configured. To access the Target Locations page, select PeopleTools, Integration Broker, Configuration, Service Configuration. In the Service Configuration tab, click the Setup Target Locations link.

  Image: Target Locations page

  This example illustrates the fields and controls on the Target Locations page. You can find definitions for the fields and controls later on this page.



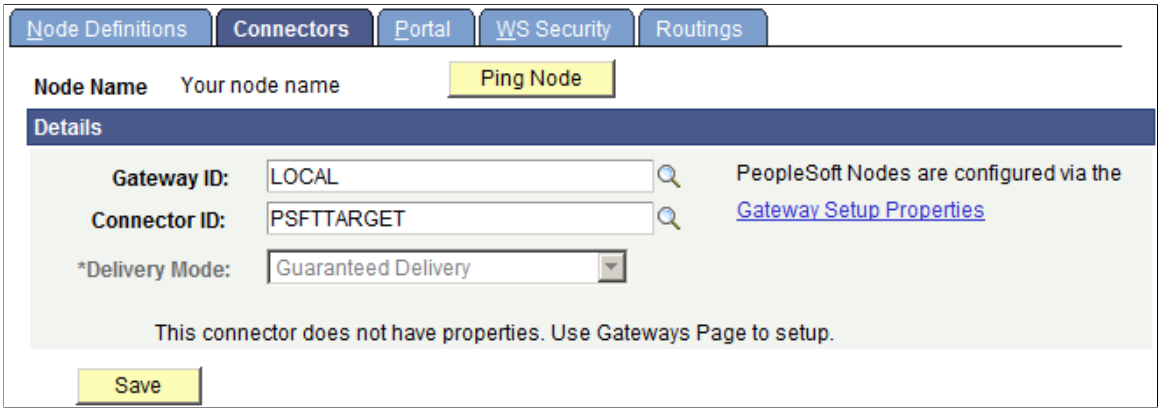
- Verify that you can ping the node. To access the Connectors page, select PeopleTools, Integration Broker, Integration Setup, Nodes, Connectors. From the Connectors page, press the Ping Node button.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Click the Ping Node button to verify the results. Make sure Message Text shows *Success.*

Image: Connectors page

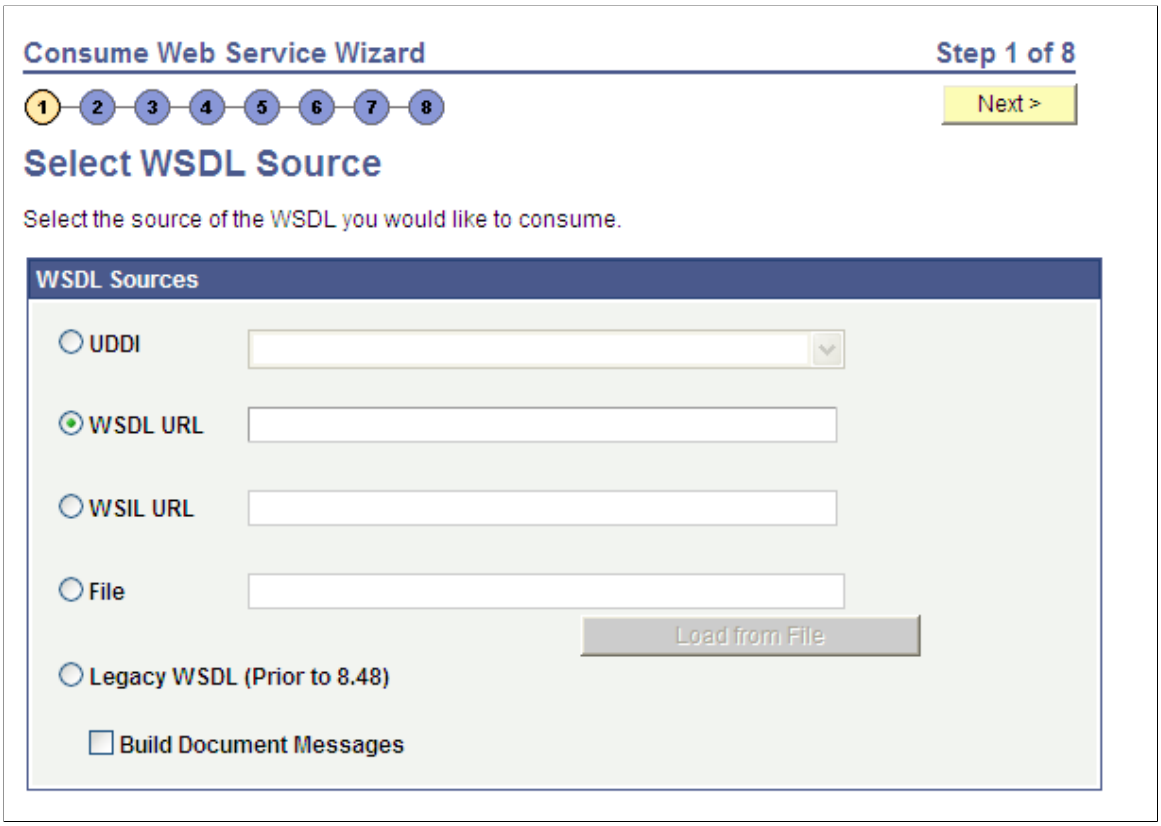
This example illustrates the fields and controls on the Connectors page. You can find definitions for the fields and controls later on this page.



- During the consume web services step ensure that the Build Documents Message check box is cleared. To access the Consume Web Services wizard, select PeopleTools, Integration Broker, Web Services, Consume Web Service.

Image: Consume Web Service Wizard page

This example illustrates the fields and controls on the Consume Web Service Wizard page. You can find definitions for the fields and controls later on this page.

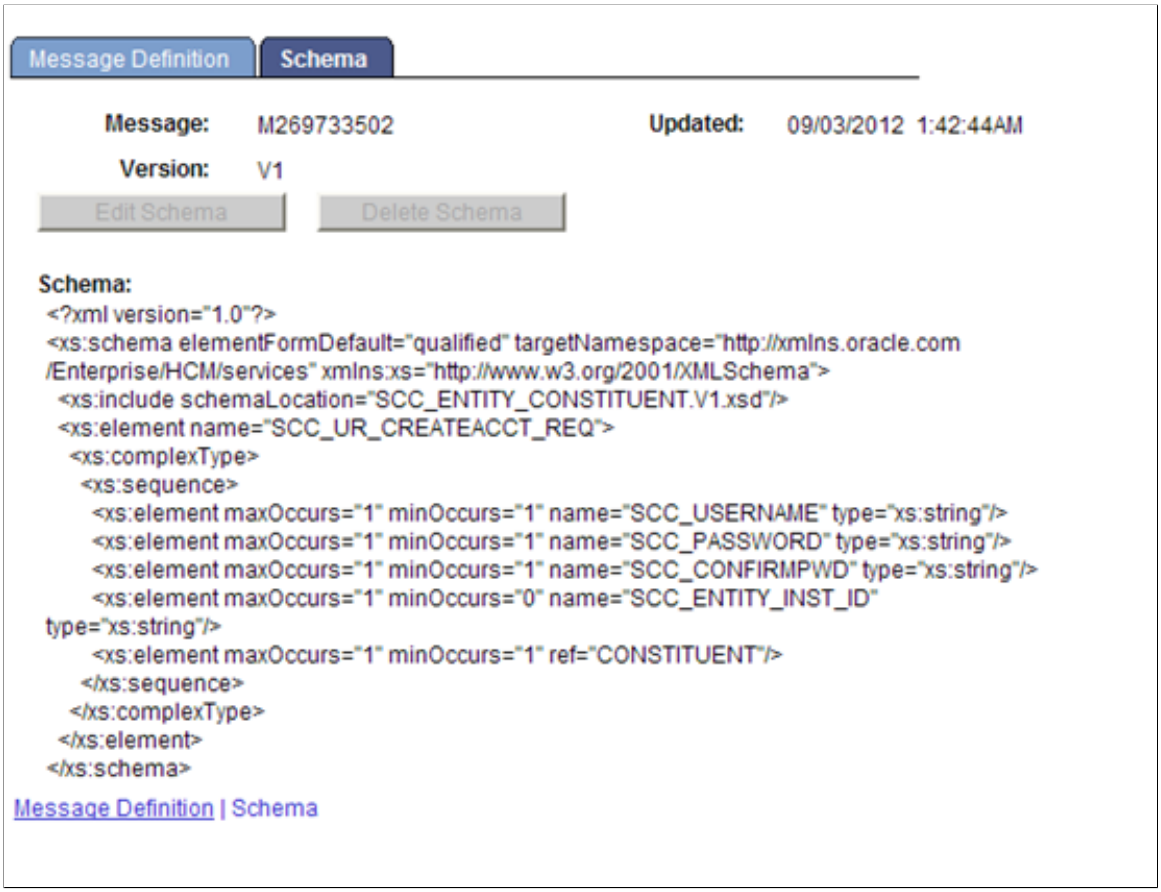


Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

- Verify that schema exists for the imported message. To access this schema, first navigate to the General page of the service operation(PeopleTools, Integration Broker, Integration Setup, Service Operations), then click the View Message link for the message, and finally click the Schema tab.

  Image: Schema page

  This example illustrates the fields and controls on the Schema page. You can find definitions for the fields and controls later on this page.



Step 6: Ensuring that the New User Registration Web Services are Running

Use the Provide Web Service page to publish the SCC_USERREG web service (PeopleTools, Integration Broker, Web Services, Provide Web Service).

New User Registration includes the SCC_USERREG web service with the following service operations:

- SCC_USERREG_AUTHENTICATE
- SCC_USERREG_CREATEACCT
- SCC_USERREG_GET_PASSWORD
- SCC_USERREG_GET_PSWD_HINT
- SCC_USERREG_GET_USERID
- SCC_CHECK_AUTH

 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Note: Activate this *only* if you use Simplified Campus Experience

See the product documentation for *PeopleSoft Integration Broker*.

Step 7: Creating a URL to Access the New User Registration Login page

The URL triggers the NUR framework. It transfers your anonymous users to your New User Registration login page. To facilitate the consumption of the NUR framework, you can use the New User Registration Installation page to automatically generate the URL. The URL is embedded with the environment information you specify as well as the logic that the NUR framework provides. For example, the autologger and gatekeeper information. You use the New User Registration Installation page, and, optionally, the New User Registration Context page to configure the NUR constants, and activate the Production or Tester URL. Use the Production URL if you are ready to deploy your online transactions, and the Tester URL to test your online transactions.

You can hardcode the URL in your applications, although it is recommended to use logic to dynamically refer to the URL. As part of the NUR framework, the application class SCC_IDENTITY_MGR.UTIL.NURConstants contains the logic to use the URL that you specify as Active in the New User Registration Context page. To see an example of how the application class is extended, see the Delegated Access application class SCC_DA.NOTIFICATION.NOTIFY.OnExecute. In this application class, the NUR context ID for Delegated Access is hardcoded: SCC_NURCTXT_20120918102441. The method ActiveAutoGenURL is implemented to retrieve the proper URL that you would include in an email message. For Delegated Access, an email message is sent to the proxies to inform them how to access the school system. It includes the URL (a hyperlink) that is also dynamically retrieved.

When you dynamically refer to the URL, it ensures that if there are any changes to the New User Registration constants, the current URL is always retrieved. It also allows you to easily switch between your Tester URL and Production URL.

See product documentation for *PeopleTools: Portal Technology*, Configuring the Portal Environment, Understanding Web Profiles.

Related Links

Defining Installation Options for New User Registration
Setting Up New User Registration Context
Understanding New User Registration

Step 8: Provisioning the Gatekeeper Permission List to all of Your Users

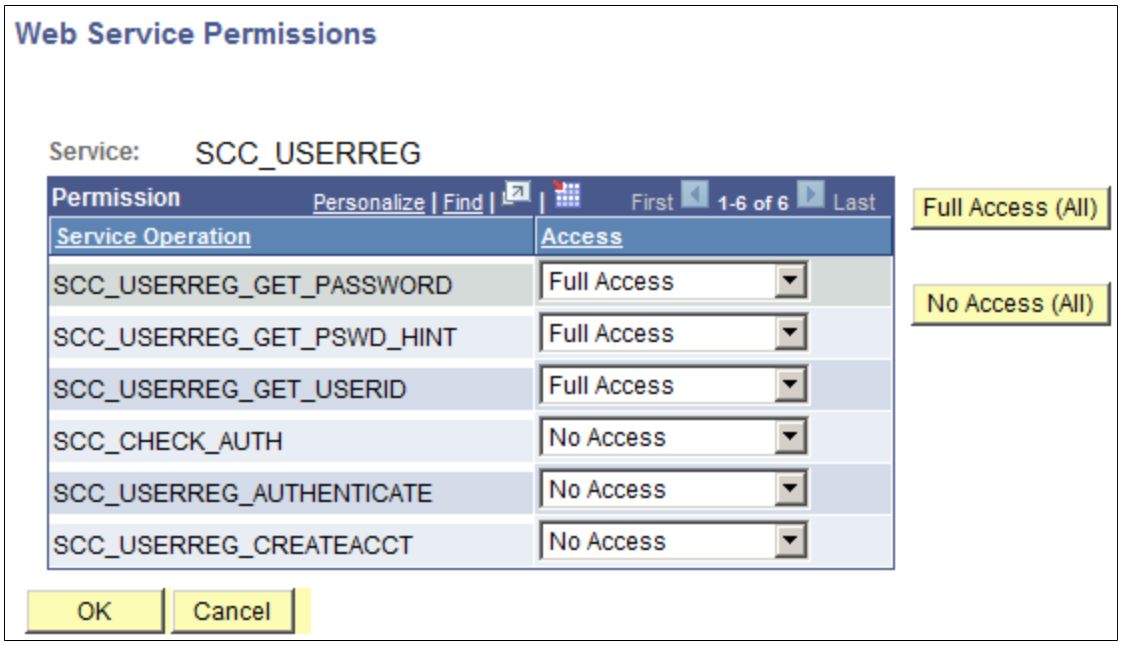
The permission list HCCPCSSA1200 - CS NUR GateKeeper is used to access the Gatekeeper. Add this permission list to a role that you want to assign to all of your users that could potentially register with your system through a New User Registration login page. For example, students, alumni, applicants, and so on.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The HCCPCSSA1200 permission list grants access to the web library WEBLIB_SCC_NUR.

Image: HCCPCSSA1200 Web Service Permissions Page

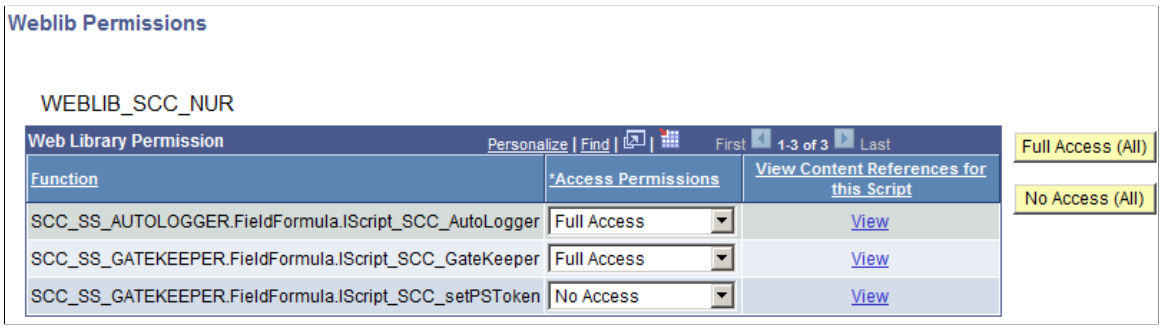
This example illustrates the fields and controls on the HCCPCSSA1200 Web Service Permissions Page.



The web library grants access to the following permissions:

Image: WEBLIB_SCC_NUR Weblib Permissions Page

This example illustrates the fields and controls on the WEBLIB_SCC_NUR Weblib Permissions Page.



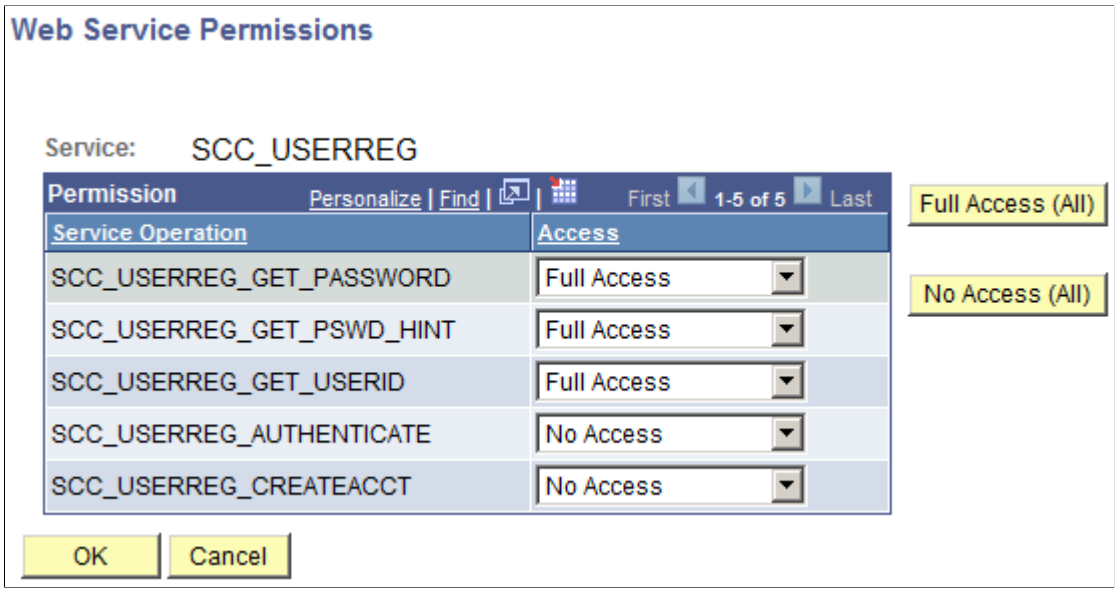
Having security access to the Gatekeeper allows your existing users to sign in through New User Registration login page with an existing user ID and password, and take advantage of the Gatekeeper functions. For example, automatic application level provisioning and page transfer after successfully signing into your system. If users do not have access to the Gatekeeper, they see the following error after they are authenticated: *Not Authorized.*

 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

If you implement the New User Registration Forgot Password and Forgot User ID utilities, your existing users also need to have access to the HCCPCSSA1210 permission list. This permission list grants access to the web services that are needed for the Forgot Password and Forgot User ID utilities.

Image: HCCPCSSA1210 Web Service Permissions Page

This example illustrates the fields and controls on the HCCPCSSA1210 Web Service Permissions Page.



For guest users, create a new role that exclusively contains the HCCPCSSA1200 permission list. Also, when you implement the New User Registration Forgot Password and Forgot User ID utilities, include the HCCPCSSA1210 permission list. Add this role to the SCC_SS_TEMPLATE user ID. By default, the guest is provisioned with all the security setup inside that user ID.

Related Links

Step 1: Initial Setup for New User Registration

Step 9: Configuring the Forgot User ID Utility

To configure the Forgot User ID Utility:

1. Store email addresses in the PSOPRDEFN.EMAILID and PSUSEREMAIL.EMAILID records where PRIMARY_EMAIL = ‘Y’.

   To take advantage of the Forgot User ID utility, all users *must* have an email address stored in their user profile. When users forget their user ID, they are asked to enter their email address. The email address is matched to the one stored in your system. This email address must match *only* one user profile stored in your system.

   You can require users that are created through the SCC_USERREG_CREATEACCT service operation to enter an email address. For example, guests who create their own account using the New User Registration login page. To require users to enter an email address, select this option in the New User Registration Installation page. The email address users enter at account creation time is automatically stored in the newly created user profile. The email address is used to populate the records PSOPRDEFN.EMAILID and PSUSEREMAIL.EMAILID with an email type (EMAILTYPE field), and the PRIMARY_EMAIL field must be selected.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

See:

- Defining Installation Options for New User Registration
- *PeopleTools: Security Administration*, "Setting General User Profile Attributes"

2. Set up the Notifications Framework.

   a. If necessary, set up the generic template NUR_EMAIL_OPRID. The generic template NUR_EMAIL_OPRID is configured for the Forgot User ID email message. You can modify the text of this template. To set up the template, go to PeopleTools, Workflow, Notifications, Generic Templates.

      See Understanding New User Registration, Notifications Framework and New User Registration.

   b. Verify the notification setup and the email recipients for the generic template. This setup is delivered with your system as sample data (Notification Template ID SCC_NTF_TMP_20130213051038 – NUR_EMAIL_OPRID). To view the setup, go to Set up SACR, System Administration, Utilities, Notifications, Notification Setup.

   c. Verify the setup for the notification consumer for New User Registration. This is delivered with your system as sample data (Notification Consumer ID SCC_NTF_CON_20121212000832 – New User Registration). To view the setup, go to Set up SACR, System Administration, Utilities, Notifications, Notification Consumer Setup.

3. Grant all users access to a permission list that is set up to grant access to the Forgot My User ID page.

   See Step 1: Initial Setup for New User Registration.

Step 10: Configuring the Forgot Password Utility

To configure the Forgot Password Utility:

1. Store email addresses in the PSOPRDEFN.EMAILID and PSUSEREMAIL.EMAILID records where PRIMARY_EMAIL = 'Y'.

   The New User Registration Forgot Password utility leverages the PeopleTools security function for forgotten passwords. This function uses the PeopleTools Workflow and requires users to have an email address stored in their user profile (General tab, Edit Email Address link).

   To take advantage of the Forgot Password utility, you can require users that are created through the SCC_USERREG_CREATEACCT service operation to enter an email address. For example, guests who create their own account using the New User Registration login page. To require users to enter an email address, select this option in the New User Registration Installation page. The email address users enter at account creation time is automatically stored in the newly created user profile. The email address is used to populate the records PSOPRDEFN.EMAILID and PSUSEREMAIL.EMAILID with an email type (EMAILTYPE field), and the PRIMARY_EMAIL field must be selected.

   See:

   - Defining Installation Options for New User Registration

 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

- *PeopleTools: Security Administration*, “Setting General User Profile Attributes”

2. Create the URL you include in the forgotten password email text.

   When you use the Forgot Password utility, the user receives an email message that contains the newly generated password. In the email message, it is recommended that you include a URL to access the New User Registration login page. Use the URL to force users to reset the temporary password they received. After users log in with their temporary password, they should be automatically redirected to the Change Password page. The URL you use must be embedded with the New User Registration context ID that grants the newly authenticated user the security to access and immediate transfer to the Change Password page. Your system includes a New User Registration Context ID sample: SCC_NURCTXT_20130211110717 - NUR_CHANGE_PASSWORD. Make sure the generic URL you use has been configured using the New User Registration Installation page.

   See:

   - Step 7: Creating a URL to Access the New User Registration Login pageDefining Installation Options for New User Registration
   - Setting Up New User Registration Context

3. Create password hint questions.

   To use the Forgot Password utility, users need to answer a security question or password hint question. To create password hint questions, go to PeopleTools, Security, Password Configuration, Forgot Password Hint.

   See *PeopleTools: Security Administration*, “Creating Hints for Forgot Passwords.”

4. Set up the Forgot Password email text.

   When the user initiates the Forgot Password utility and successfully answers the security question, an email message is sent to the email address that is stored in the user's profile. It includes a newly generated password. You can configure the email message text by going to PeopleTools, Security, Password Configuration, Forgot Password Email text.

   The email text must include the `<<%PASSWORD>>` tag. PeopleTools replaces the tag with the newly generated password. To facilitate user experience, it is recommended that you also include a URL that transfers the user automatically to the New User Registration sample login page (or your own version of this page). This is the URL you create in step 2. This forces the user to immediately change the newly received password. The PeopleTools email text editor allows you to easily paste a URL. You can use the URL you marked as *Active* in the New User Registration context ID in your system (SCC_NURCTXT_20130211110717 - NUR_CHANGE_PASSWORD).

   This is an example of an email text:

   You are receiving this auto-generated email message because you requested your Campus Solutions password to be reset. Use the following temporary password: <<%PASSWORD>>. Click this link or copy the below URL to access the system with your newly generated password. You will be requested to change the temporary password immediately.” https://yourKioskServer.yourKioskDomain.com/psc/ps/EMPLOYEE/HRMS/c/SCC_NUR.SCC_NUR_REG.GBL=start?CAMPUS_URL=https%3a%2f%2fyourCSServer.yourCSDomain.com%2fpsc%2fps%2fEMPLOYEE%2fHRMS%2fs

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

%2fWEBLIB_SCC_NUR.SCC_SS_GATEKEEPER.FieldFormula.IScript_SCC_GateKeeper %3fSCC_APPL_CONTXT_ID%3dSCC_NURCTXT_20130211110717

See *PeopleTools: Security Administration*, "Working with Passwords."

5. Grant all your users access to a self-service page where they can respond to a security question.

   Delivered with your system with the generic PeopleTools security a self-service user can answer is a security question under Home page, My System Profile. In the General Profile Information page (USER_SELF_SERVICE), by clicking the link Change or set up forgotten password help, the user can select a question and enter a response. This page is delivered with your system and security needs to be granted to all of your users. Alternatively, a simpler self-service version of this page could be created.

6. Configure the Forget My Password page.

   This is a delivered custom version of the Tools page EMAIL_PSWD as public.

   See *PeopleTools: Security Administration*, "Working with User Profiles Across Multiple PeopleSoft Databases, Implementing Default User Profile Synchronization."

7. Make sure you grant all your users access to a permission list set up with Allow Password to be Emailed and Forgot My Password.

   See Step 1: Initial Setup for New User Registration.

8. Set up the New User Registration context ID for the Change My Password page, or use the SCC_NURCTXT_20130211110717 - NUR_CHANGE_PASSWORD context ID.

9. Set the PeopleTools Workflow to activate email.

   The New User Registration Forgot Password utility leverages the PeopleTools send password functionality. Because this functionality uses the PeopleTools Workflow, the following setup is required:

   a. Go to PeopleTools, Workflow, Defaults & Messages, Set Workflow Defaults.

   b. In the Worklist System Defaults page, System Wide Route Processing make sure the Worklists Active and the Email Active checkboxes are selected.

   c. Reboot the application server for the changes to take effect.

Troubleshooting New User Registration

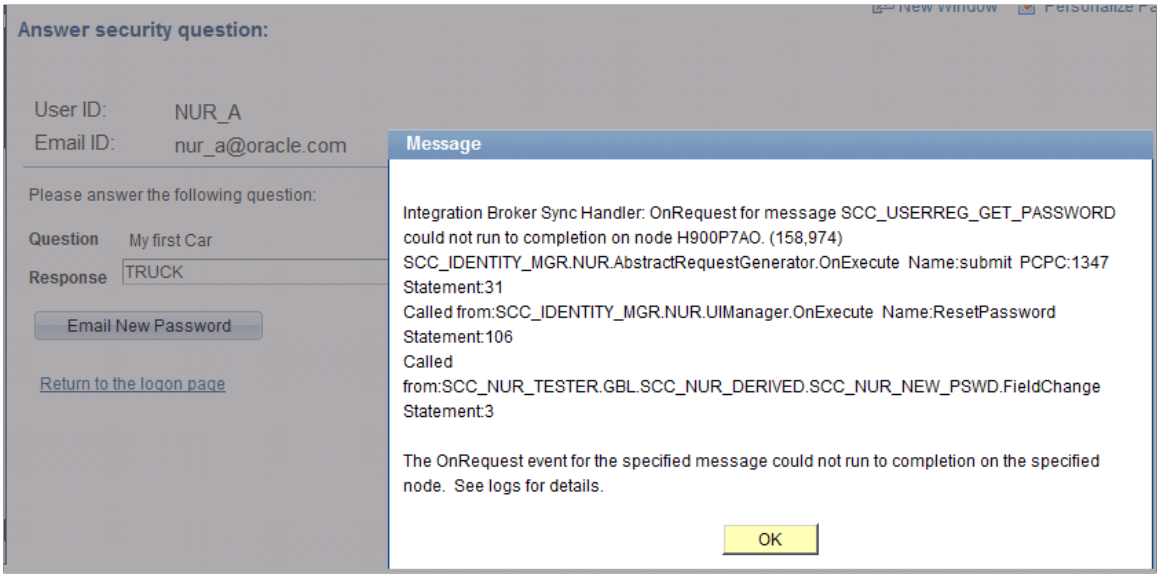
- Ensure that the service operations created for the consuming self-service transactions and the service operations delivered with the New User Registration framework are configured with Full Access security. To do so, access the General page (PeopleTools, Integration Broker, Integration Setup, Service Operations, General) for the desired service operation. Click the Service Operation Security link and make sure the permission lists used inside SCC_SS_TEMPLATE have Full Access.

 Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

- If you use the New User Registration Forgot Password utility and you see the following Integration Broker error, it means your user does not have access to a permission list set to 'Allow Password to be Emailed = 'Y':

  Image: Integration Broken error

  This example illustrates the fields and controls on the Integration Broken error. You can find definitions for the fields and controls later on this page.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.