



EmpowHR: Section 2 - User Security



PUBLICATION CATEGORY
HR and Payroll Processing

PROCEDURE MANUAL
EmpowHR

SECTION 2
User Security

Table of Contents

EmpowHR User Security (HD)	1
Distributed Security Administrator	3
Granting Roles and Row-Level Permission Lists	4
Creating a Row-Level Permission List.....	6
Create New Oprid	7
Employee Password Reset	7
Permission Lists Overview	8
Roles	9
User Profiles	9
Security Administrator Role	11
Creating a Distributed Security Administrator Role	11
Defining Roles That the Distributed Security Administrator Can Grant	12
Assigning the Distributed Security Administrator Roles to a User	13
People Tools	15
User Profiles (People Tools)	15
Create and Maintain User Profiles	16
Copy User Profiles	24
Delete User Profiles.....	26
Distributed User Profiles	27
Distributed User Set Up.....	29
Purge Inactive User Profiles	29
Permissions and Roles	31
Permission Lists	31
Copy Permission Lists	57
Delete Permission Lists	59
Roles Component	60
Copy Roles.....	70
Delete Roles.....	71
Execute Role Rules	73
Password Configuration	73
Password Controls.....	74
Forgotten Password Email Text.....	77
Forgotten Password Hint	79
Delete Forgotten Password Hint	80
Security Objects	82

User Profile Types.....	82
Tables to Skip	84
Security Links	85
Digital Signature	87
Single Signon	90
Signon PeopleCode	91
Query Security.....	92
Query Access Manager.....	93
Query Access List Cache.....	95
Common Queries	96
Mass Change Operator Security	97
Tree Manager.....	101
Introduction to Tree Manager	102
Tree Viewer	106
Tree Auditor	108
Tree Structure.....	110
Tree Utilities.....	112
Copy/Delete Tree	113
Export Tree	115
Import Tree	117
Repair Tree	120
Repair Tree Reports.....	122
Index	125

EmpowHR User Security (HD)

Security is critical for core business applications. Typically, not every group in the organization should have access to all of the application features or have access to all the data within the application.

EmpowHR provides security features to ensure that an Agency's sensitive application data does not fall into the wrong hands.

The application security menu can apply to all users, including employees, managers, customers, and contractors. Users are grouped according to defined roles to give them different degrees of access.

EmpowHR also enables the Agency to restrict user access to records/data within a menu selection. Thus, a Security Administrator can limit a user's access to only records/data that belong in those organizational codes (Department Identification (DEPTID)) associated with a specifically defined Row-Security Permission List. This data access level is defined for each user in each user's individual profile by the Row-Security Permission List that is assigned to that profile. The Security Administrator is at the highest level in the Department Tree (Organizational Structure, Table Management System (TMGT), Table 005, Agency Organizational Structure). A Security Administrator can delegate all or part of security functions to a person(s) which is called a Distributed Security Officer. The Distributed Security Officer's access could be limited to a specific Agency within the Department Tree.

EmpowHR DEPTIDs are used in place of the National Finance Center (NFC) Organizational Codes and are required for various types of transactions within the application. Prior to data being loaded into *EmpowHR*, these DEPTIDs must be established in order to translate each unique NFC Organizational Code for organizations into unique *EmpowHR* DEPTIDs.

Also, prior to the Agency data being loaded into *EmpowHR* and based on information the Agency has provided, a security tree is created that represents the Agency's organization security hierarchy. Security trees enable that Agency to grant (or deny) access to an employee's data by granting access to the entity (DEPTIDs) to which the user reports. To grant access to a group of entities (DEPTIDs), grant access to the entity (DEPTID) within the security tree to which all of those entities report. Access can be restricted to individual entities or to a group of entities. The security definition and hierarchy are described as follows:

- A security definition refers to a collection of related security attributes that are created using PeopleTools Security. The three main *EmpowHR* security definition object types are:
 - User Profiles
 - Roles
 - Permission Lists

Because implementing applications to the Internet considerably increases the number of potential users, the application must accommodate an efficient method of granting authorization to varying user types. Security definitions provide a modular means to apply security attributes in a scalable manner.

Each user of the application has an individual User Profile, which in turn is linked to one or more Roles. To each Role, one or more Permission Lists are assigned. These Permission Lists ultimately control which pages a user is able to access. Thus a user inherits permissions by way of a role. Permissions being assigned directly to a user's profile are an exception to this rule. The following table provides a summary of each profile and the description of each:

User	Description
Super User	This user understands the setup of the application and has access to the defined business rules area of the application. In addition, they have full access to all data entry pages, correction-mode capabilities to modify historical data, and the capability to run all processes within their application. This user is considered the application expert.
Lead User	This user has full access to all data entry pages, correction-mode capabilities to modify historical data, and the capability to run most processes within the application.
Average User	This user has access to a limited number of pages and processes within the application. If there are more than five categories in this area, it is divided into multiple roles. This area includes users that perform tasks such as approving, entering data, updating existing data, and processing.
Data Entry	This user has access to a very limited number of pages within a component. The data entry user has access to add or submit data but is unable to update the record. This role is not often used due to the restrictiveness.
Inquiry	This user has access to some pages of the application in a read-only mode. They also have access to standard inquiry pages and report-generation areas within the application.

EmpowHR security restrictions are applied to the following components in order to protect the application and data:

- Reporting
- Inquiry
- Transaction processing
- Process running
- System access
- User IDs
- Sign-on and timeout security

The following table provides a summary of each component and the restrictions that may be applied to each.

Component	Security Description
Reporting	Limits users from reporting on data from organizations or Departments they are not part of or for which they cannot conduct transactions. Access is limited via business unit and Department role.
Inquiry	Allows security set up through Departmental roles for read-only access to certain data entry or transaction pages and online inquiry pages with predefined search capabilities. <i>EmpowHR</i> query tool allows security control at table-level security, row-level security, field-level security, and run only.
Transaction Processing	Assigns data entry and transaction processing limited to security based on user roles in <i>EmpowHR</i> . Allows user to perform data entry and transaction processing for the areas that have been authorized.
Running Processes	Utilizes process groups based on Departmental business roles to limit access to running certain processes.
External Process	Gains user access to the application remotely via the Internet with appropriate authentication.
User ID	Allows users security configuration to access applications and be able to move between them without having to log in and out.
Sign-on Time	Allows adjustable intervals for a user to access the application or sign on to <i>EmpowHR</i> .
Timeout	Specifies the amount of time the user's machine can remain idle before <i>EmpowHR</i> automatically disconnects the user from the application so they cannot gain access.

This section includes the following topics:

Distributed Security Administrator	3
Create New Oprid.....	7
Employee Password Reset	7
Permission Lists Overview	8
Roles	9
User Profiles.....	9

Distributed Security Administrator

This section will explain the process for the Distributed Security Administrator to grant Roles and Row-Level Permission Lists to an operator identification (OPRID) (user).

For more information see:

Granting Roles and Row-Level Permission Lists4
Creating a Row-Level Permission List.....6

Granting Roles and Row-Level Permission Lists

Below is the step-by-step process for the Security Administer to grant Roles and Row-Level Permission Lists to the Distributed Security Administrator for administration:

1. Select the **Peoples Tools** menu group.
2. Select the **Security** menu.
3. Select the **User Profiles** menu item.
4. Select the **Distributed User Profiles** component. The Distributed User Profile page - Find an Existing Value tab is displayed.

Distributed User Profile

Enter any information you have and click Search. Leave fields blank for a list of all values.

Find an Existing Value Add a New Value

▼ Search Criteria

Search by: UserID ▼ begins with

Figure 1: Distributed User Profile Page - Find an Existing Value Tab

5. Enter the applicable search criteria.
6. Click **Search**.
7. Select a Role Name from the search criteria.

- Select the **User Roles** tab. The Distributed User Profile page - User Roles tab is displayed.



Figure 2: Distributed User Profile Page - User Roles Tab

- Click **+** to add an additional Role.
- Click the look-up icon to display the roles that the Distributed Security Administrator can grant. The roles that the Distributed Security Administrator can grant are defined by the Security Administrator.
- Select the applicable Role Name.
- Click **Save**.
- Select the **General** tab. The Distributed User Profile page - General tab is displayed.

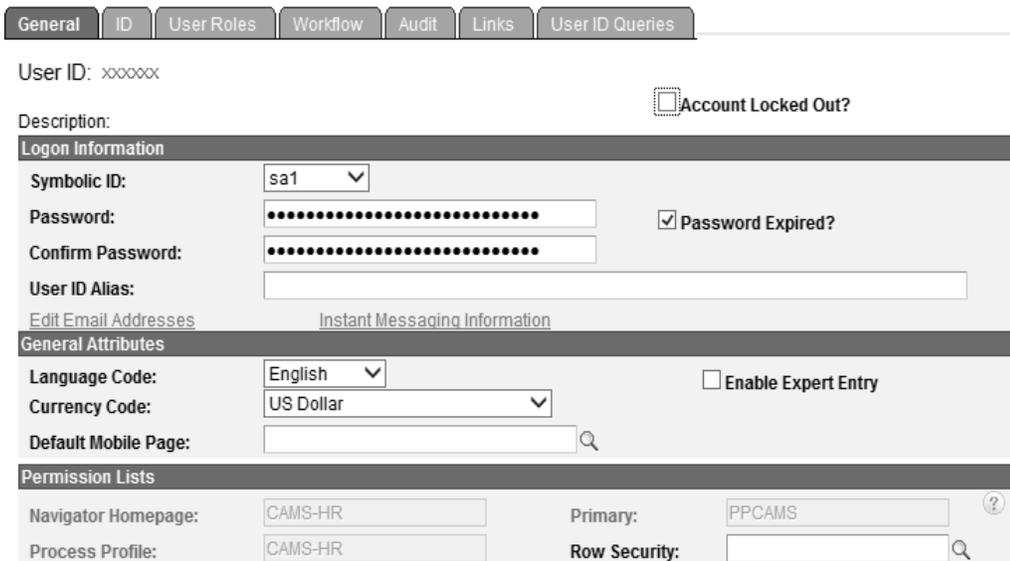


Figure 3: Distributed User Profile Page - General Tab

- Click the look-up icon next to the Row Security field to display Permission List(s).

15. Select the applicable Permission List. This field grants access to the user ID in order to view data in a component within the application.
16. Click **Save**.

Creating a Row-Level Permission List

Below is the step-by-step process that will allow the Security Administrator to create a Row-Level Permission List for the Distributed Security Administrator for administration (access to the data within a component).

1. Select the **Peoples Tools** menu group.
2. Select the **Security** menu.
3. Select the **Permissions & Roles** menu item.
4. Select the **Permission Lists** component. The Permission Lists page - Find an Existing Value tab is displayed.

Permission Lists

Enter any information you have and click Search. Leave fields blank for a list of all values.

Find an Existing Value Add a New Value

▼ Search Criteria

Search by: Permission List ▼ begins with

Figure 4: Permission Lists Page - Find an Existing Value Tab

5. Enter the applicable search criteria.
6. Click **Search**.

7. Select the **Add a New Value** tab. The Permission Lists page - Add a New Value tab is displayed.

Permission Lists



The screenshot shows a web interface with two buttons: 'Find an Existing Value' and 'Add a New Value'. The 'Add a New Value' button is highlighted. Below the buttons is a text input field labeled 'Permission List:'.

Figure 5: Permission Lists Page - Add a New Value Tab

8. Enter the name of the new permission list.
9. Click **Add**.
10. Click **Save**. The new permission list is saved.

Create New Oprid

To Create a New Oprid:

1. Select the **EmpowHR User Security (HD)** menu group.
2. Select the **Create New Oprid** component.

Note: When the **Create New Oprid** component is selected from the **EmpowHR User Security (HD)** menu group, the user is rerouted to the **PAR Processing** menu group, **Create New Oprid** component. The completion of this component is the same from either menu group. For more information on Create New Oprid, refer to the **PAR Processing** section, **Create New Oprid** topic.

Employee Password Reset

To access the Employee Password Reset page:

1. Select the **EmpowHR User Security (HD)** menu group.
2. Select the **Employee Password Reset** component.

Note: When the **Employee Password Reset** component is selected from the **EmpowHR User Security (HD)** menu group, the user is rerouted to the **PAR Processing** menu group, **Employee Password Reset** component. The completion of this component is the same from either menu group. For more information on Employee Password Reset, refer to the **PAR Processing** section, **Employee Password Reset** topic.

Permission Lists Overview

Permission lists are the building blocks of user security authorizations. Create permission lists before roles and user profiles are created. When defining permission lists, however, consider the roles, data, and user profiles that the Agency will use. Remember that roles are intermediary objects between permission lists and users. The Agency uses roles to automatically assign application permissions to users.

Application permission lists may contain a variety of accessibilities (i.e, sign-in times) and view/update/add page access authority. Application permission lists are more flexible and scalable when they contain fewer permissions but require more effort to maintain. It is very important to have a balanced approach when establishing these guidelines.

EmpowHR enforces data permission security with security search views. To understand how this is done, it helps to understand how *EmpowHR* retrieves data when the user accesses a menu selection. When the user opens a menu selection in *EmpowHR*, a search page is displayed. The search page represents the search record, and the fields that appear are the search keys and alternate key fields that uniquely identify each row of data. *EmpowHR* uses the information that the user enters to retrieve the data that the user wants to view or enter/update information. A search page may have EmplID as a key field and Name as an alternate key. (For example: if the user enters Smith in the Name field, *EmpowHR* retrieves all the data rows with the Name field data that matches Smith.) *EmpowHR* also uses search records to enforce data permission security. Search views for menu selections that contain sensitive data also contain a security view to control data access. *EmpowHR* adds the user's security profile, including their user ID and the value of the Row-Level Security Permission List attached to their user profile. The SQL (Structured Query Language) selects the statement along with the values that the user entered on the search page. *EmpowHR* retrieves the data that matches the criteria from the search page and the user's data Row-Level Security Permission List. *EmpowHR* does not retrieve data for people to whom you have not granted the user's Row-Level Security Permission List data access to.

The permission list relationship to the Department Security Tree is what defines the permission list as a Row-Security Permission List. Set Identifications (SETID), associated DEPTIDs, and Access Codes are what set apart a Row-Level Security Permission List from a standard application Permission List. The SETID determines the Tree, the DEPTID determines the position on the Tree, and the Access Code designates whether or not the DEPTID is accessible or blocked, thus providing the translational information for the user profiles access to data via the Row-Level Security Permission List and the organizations Department Security Tree.

To create, maintain, copy, and delete permission lists:

1. Select the *EmpowHR User Security (HD)* menu group.
2. Select *Permission Lists*.

Note: When the **Permission Lists** component is selected from the **EmpowHR User Security (HD)** menu group, the user is rerouted to the **People Tools** menu group, **Permission Lists** component. The completion of this component is the same from either menu group. For more information on **Permission Lists**, refer to the People Tools section, Permission Lists topic.

Roles

Roles are intermediate objects that usually link user profiles to application permission lists. The Agency can assign multiple Roles to a user profile and can assign multiple application permission lists to a role. Roles are essentially used to group users by the specific tasks they perform.

Non-permission list-based roles link user profiles directly to groups of users without any inherited menu access within *EmpowHR*.

This option is used to create and maintain roles established in the database. For more information about Roles, refer to **People Tools** (on page 15) and **Permissions and Roles** (on page 31) in this procedure.

To create and maintain roles:

1. Select the **EmpowHR User Security (HD)** menu group.
2. Select the **Roles** component.

Note: When the **Roles** component is selected from the **EmpowHR User Security (HD)** menu group, the user is rerouted to the **People Tools** menu group, **Roles** component. The completion of this component is the same from either menu group. For more information on Roles, refer to the **People Tools** (on page 15) topic or the **Permissions and Roles** (on page 31) topic.

User Profiles

User profiles define individual *EmpowHR* users. User profiles are defined and then linked to one or more roles. Typically, a user profile must be linked to at least one role to be a usable profile. The majority of values that make up a user profile are reinherited from the linked roles.

It is possible to have a user profile with no roles. This might be a user who is not allowed access to *EmpowHR*; however, workflow-generated email will be sent to the user.

Define user profiles by entering the appropriate values on the user profile pages. The user profile contains values that are specified by the user, such as a user password, an email address, an employee ID, etc.

The **User Profiles** option is used to establish user profiles. User profiles can also be copied, deleted, distributed and purged from this option.

To create and maintain user profiles:

1. Select **EmpowHR User Security (HD)** menu group.
2. Select **User Profiles** component.

Note: When the **User Profiles** component is selected from the **EmpowHR User Security (HD)** menu group, the user is rerouted to the **People Tools** menu group, **User Profiles** component. The completion of this component is the same from either menu group. For more information on **User Profiles**, refer to **User Profiles (People Tools)** (on page 15).

Security Administrator Role

This section provides the Security Administrator with a step-by-step guide for the changes to the Security 9.0.

For more information see:

- Creating a Distributed Security Administrator Role 11
- Defining Roles That the Distributed Security Administrator Can Grant 12
- Assigning the Distributed Security Administrator Roles to a User 13

Creating a Distributed Security Administrator Role

This component is used by the Security Administrator (Super User) to create a new role in *EmpowHR*. This role is created for the Distributed Security Administrator (SubAgency Administrator).

The following describes the procedure for adding roles:

1. Select the **Peoples Tools** menu group.
2. Select the **Security** menu.
3. Select the **Permissions & Roles** menu item.
4. Select the **Roles** component. The Roles page - Add a New Value tab is displayed.

Roles



Figure 6: Roles Page - Add a New Value Tab

5. Enter the Role Name.

- Click **Add**. The Roles page - General tab is displayed.

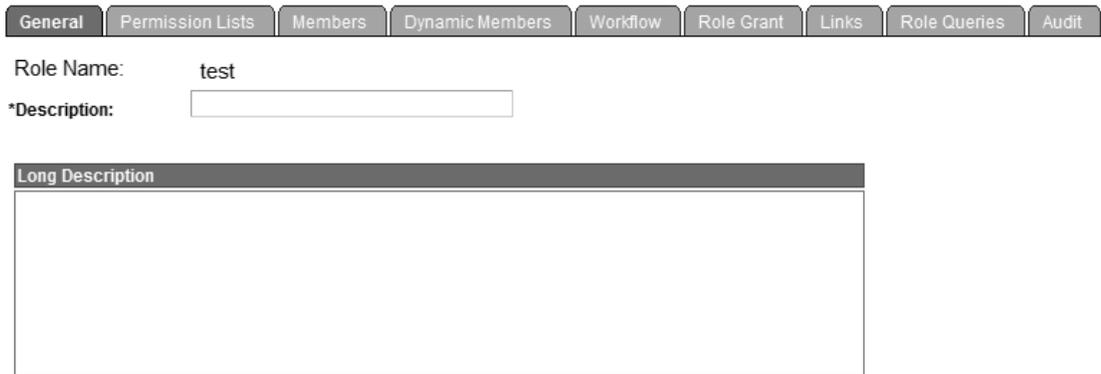


Figure 7: Roles Page - General Tab

- Enter the description of the role.
- Click **Save**.

Defining Roles That the Distributed Security Administrator Can Grant

Below is a step-by-step process that allows the Security Administrator to assign a role(s) that the Distributed Security Administrator role will be able to grant.

- Select the **Peoples Tools** menu group.
- Select the **Security** menu.
- Select the **Permissions & Roles** menu item.
- Select the **Roles** component. The Roles page - Find an Existing Value tab is displayed.

Roles

Enter any information you have and click Search. Leave fields blank for a list of all values.

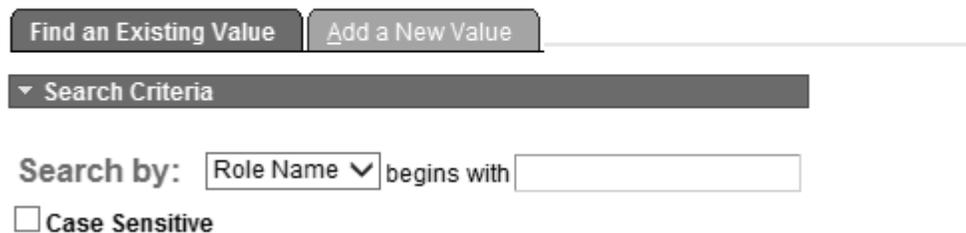


Figure 8: Roles Page - Find an Existing Value Tab

- Enter the applicable search criteria.

Note: If no information is entered, click the search icon for a list of values.

6. Click **Search**.
7. Select a value.
8. Select the **Role Grant** tab. The Roles page - Role Grant tab is displayed.

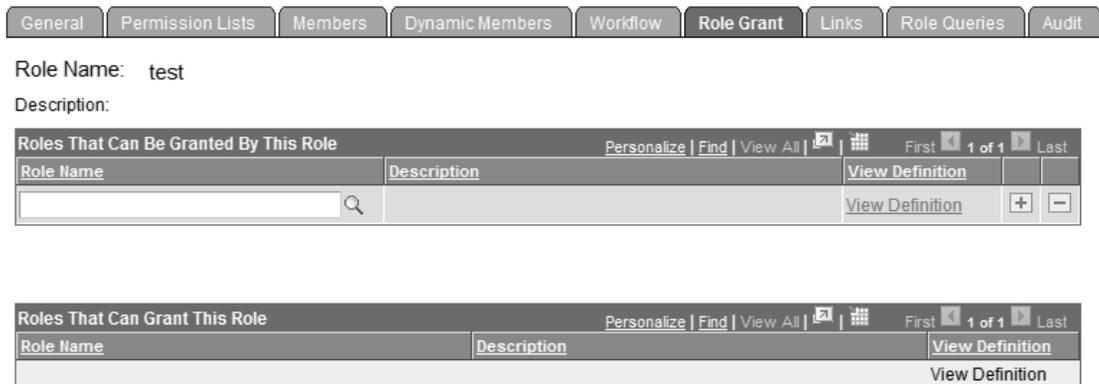


Figure 9: Roles Page - Role Grant Tab

9. Enter the Role Name in the Roles That Can Be Granted By This Role section.
10. Click the look-up icon.
11. Click **Search**.
12. Select a value.
13. Click **Save**.

Note: Select the **Members** tab to display a list of user IDs that have the selected role.

Assigning the Distributed Security Administrator Roles to a User

Below is a step-by-step process for the Security Administrator to assign the Distributed Security Administrator role to an Operator ID (OPRID).

1. Select the **Peoples Tools** menu group.
2. Select the **Security** menu.
3. Select the **User Profiles** menu item.

4. Select the **User Profiles** component. The User Profiles page - Find an Existing Value tab is displayed.

User Profiles

Enter any information you have and click Search. Leave fields blank for a list of all values.

Figure 10: User Profiles Page - Find an Existing Value Tab

5. Enter the applicable search criteria.

Note: If no information is entered, click **Search** for a list of values.

6. Click **Search**.
7. Select the **Roles** tab. The User Profiles page - Roles tab is displayed.

Role Name	Description	Dynamic	Route Control	View Definition
CAMS Employee	CAMS Employee	<input checked="" type="checkbox"/>	Route Control	View Definition +
PeopleSoft User	PeopleSoft User	<input checked="" type="checkbox"/>	Route Control	View Definition +

Figure 11: User Profiles Page - Roles Tab

8. Click **+** to add a new row. A new blank row is added.
9. Click the look-up icon. A list of available roles is displayed on the Look Up Role Name page.
10. Select the Role Name from the look-up results. The Role Name selected is displayed on the new row.
11. Click **Save**. The new row is saved.

People Tools

This section includes the following topics:

User Profiles (People Tools)	15
Permissions and Roles	31
Password Configuration	73
Security Objects	82
Query Security	92
Common Queries	96
Mass Change Operator Security	97

User Profiles (People Tools)

User profiles define the individual *EmpowHR* user access. The Agency defines user profiles and then links them to one or more roles. A user's profiles must be linked to at least one role in order to be a valid profile. The majority of values that make up a user profile are inherited from the linked roles.

The Agency defines user profiles by entering the appropriate value on the user profiles pages. The user profile contains values that are specific to users, such as a user password, an email address, a Row-Security Permission List, and an employee ID.

The user ID and description appear at the top of each page to help recall which user profile the user is viewing or modifying as the Agency moves through the pages.

The **User Profiles** option is used to establish user profiles. User profiles can also be copied, deleted, distributed, and purged by using this option.

For more information see:

Create and Maintain User Profiles	16
Copy User Profiles	24
Delete User Profiles	26
Distributed User Profiles	27
Distributed User Set Up	29
Purge Inactive User Profiles	29

Create and Maintain User Profiles

To create and maintain user profiles:

1. Select the **People Tools** menu group.
2. Select the **User Profiles** component. The User Profiles page - Find an Existing Value tab is displayed.

User Profiles

Enter any information you have and click Search. Leave fields blank for a list of all values.

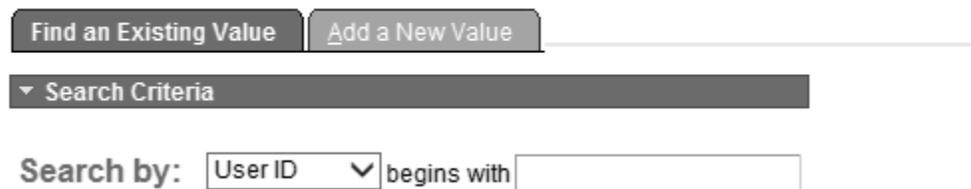


Figure 12: User Profiles Page - Find an Existing Value Tab

3. Enter the applicable search criteria.
4. Click **Search**. The User Profiles page - General tab is displayed.

OR

Select the **Add a New Value** tab. The User Profiles page - Add a New Value tab is displayed.

User Profiles



Figure 13: User Profiles Page - Add a New Value Tab

5. Complete the field as follows:

User ID Enter the user ID.

6. Click **Add**. The User Profiles page - General tab is displayed.

Figure 14: User Profiles Page - General Tab

7. Complete the fields as follows:

- | | |
|----------------------------|---|
| User ID | Populated based on the user ID entered on the User Profiles page - Add a New Value tab. |
| Account Locked Out? | Click this field if a user's account is locked. |
| Description | Populated based on the Description entered on the User Profiles page - Add a New Value tab. |
| Logon Information | |
| Symbolic ID | Select the applicable Symbolic ID from the drop-down list. |
| Password | Enter the password in this field. |
| Password Expired? | Click this field if the password has expired. |
| Confirm Password | Re-enter the password entered in the Password field to confirm the password. |
| User ID Alias | Enter the applicable user ID alias. |
| General Attributes | |
| Language Code | Defaults to English . To change, select data from the drop-down list. |
| Enable Expert Entry | Click this field to enable expert entry. |
| Currency Code | Defaults to US Dollar . Select a currency code from the drop-down |

list.

Default Mobile Page

Enter the applicable mobile information in this field or select data by clicking the search icon.

Permission Lists

Navigator Homepage

Populated and cannot be changed.

Primary

Populated based on the description entered on the User Profiles page - Add a New Value tab.

Process Profile

Populated and cannot be changed.

Row Security

Enter the applicable position name or select data by clicking the search icon.

8. Click the **Edit Email Addresses** link to add or modify email addresses if applicable.
9. Select the **ID** tab. The User Profiles page - ID tab is displayed.

Figure 15: User Profiles Page - ID Tab

10. Complete the fields as follows:

User ID

Populated based on the search/add criteria.

Description

Populated based on the search/add criteria.

ID Types and Values

***ID Type**

Click the down arrow to select the ID type. Valid values are **Employee** and **None**.

- Attribute Name** Populated with the EmplID if **Employee** is selected in the ID Type field. Click the link to sort this list by Attribute Name.
- Attribute Value** Enter the applicable name or select data by clicking on the search icon. Click the link to sort this list by Attribute Value.
- Description** Populated. Click the link to sort this list by Description.
- User Description**
- Description** Enter the user description in this field.

11. Select **Roles**. The User Profiles page - Roles tab is displayed.

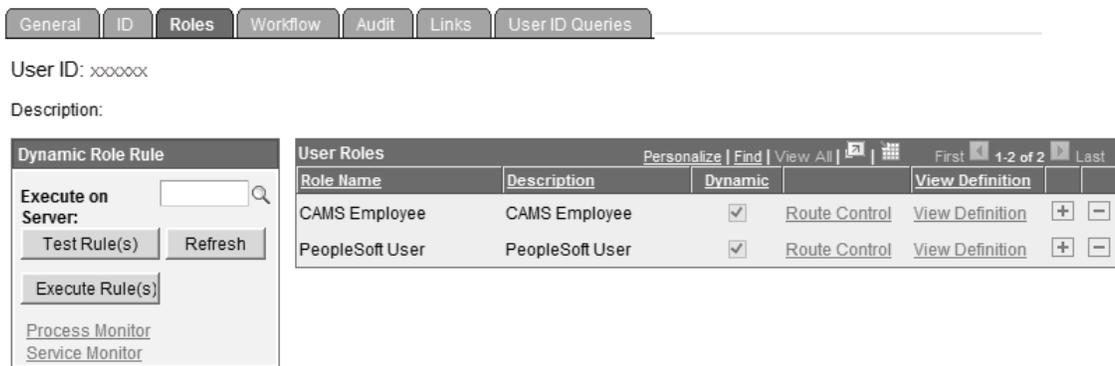


Figure 16: User Profiles Page - Roles Tab

12. Complete the fields as follows:

- User ID** Populated based on the search/add criteria.
- Description** Populated based on the search/add criteria
- Dynamic Role Rule**
- Execute on Server** Enter the server name or select data by clicking the search icon.
- Role Name** Enter the applicable role or select data by clicking the search icon. Click the link to sort the list by Role Name.
- Description** Populated based on the role enter or selected in the Role Name. Click the link to sort the list by Description.
- Dynamic** Check box if applicable. Click the link to sort the list by Dynamic.
- View Definition** Click the link to sort the list by Definition.

13. Click the **Route Control** link. The User Route Control Profiles page is displayed.

User Route Control Profiles



Figure 17: User Route Control Profiles Page

14. Complete the fields as follows:

Role Name	Populated.
*Route Control Profile	Enter the applicable information or select data by clicking the search icon.

15. Click **OK**.

OR

Click **Cancel** to return to the User Profiles page - Roles tab.

16. Click the **View Definition** link to view the definition. This field cannot be viewed if there is unsaved data on the page. Save all entries before accessing this field.

17. Select the **Workflow** tab. The User Profiles page - Workflow tab is displayed. On this page the Administrator can:

- Select an alternate user to receive routing sent to this user. Use this option when the user is temporarily out (vacation or leave). If the Alternate User ID edit box contains a user name, the system automatically forwards the new work list items to the alternate user once the profile is saved, if the From and To date range is completed.

Note: It does not reassign items already in the user's work list.

- Reassign pending work for a user if positions change or the user is temporarily out, such as on leave or on vacation. If a user has work items waiting (if indicated by the total pending work list Entries circled in red), select this check box and select the user to whom work items should be forwarded from the drop-down list. When saved, the system reassigns all existing work list entries to the specified user and the Total pending Work list Entries value changes to zero.

- Specify which types of routing a user can receive. The routing Preferences box shows the two places where the system can deliver work items: to a work list or to an email mailbox. If the user does not have access to one or both of these places, clear the check box.

Figure 18: User Profiles Page - Workflow Tab

18. Complete the fields as follows:

User ID	Populated based on the User ID used in the search/add criteria.
Description	Populated based on the Description used in the search/add criteria.
Workflow Attributes	
Alternate User ID	Enter the alternate user ID for a user or select data from the drop-down list.
Routing Preferences	
Worklist User	Check this box if the user is a worklist user.
Email User	Check this box if the user is an email user.
From Date	Enter the from date in MM/DD/YYYY format or select a date from the calendar icon.
To Date	Enter the to date in MM/DD/YYYY format or click the icon to select a date from the calendar icon.
Reassign Work	
Reassign Work To	Check this box to reassign work to another user. If this field is checked, enter the applicable user or select data by clicking the search icon.
Total Pending Worklist Entries	Populated with the number of pending worklist entries.

19. Select **Audit**. The User Profiles page - Audit tab is displayed. The Audit tab is displayed only and enables the Administrator to determine when a profile was last updated and/or who updated the profile.

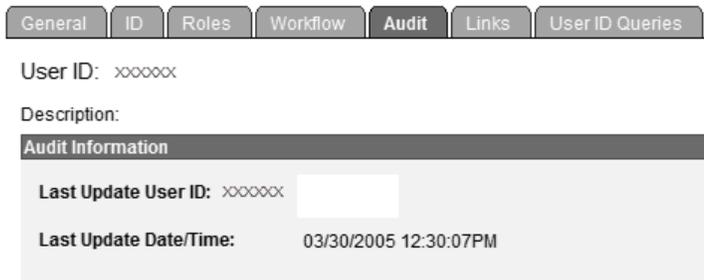


Figure 19: User Profiles Page - Audit Tab

20. Complete the fields as follows:

User ID	Populated based on the user ID entered on the search/add criteria.
Description	Populated based on the Description entered on the search/add criteria.
Audit Information	
Last Update User ID	Populated.
Last Update Date/Time	Populated.

21. Select **Links**. The User Profiles page - Links tab is displayed.

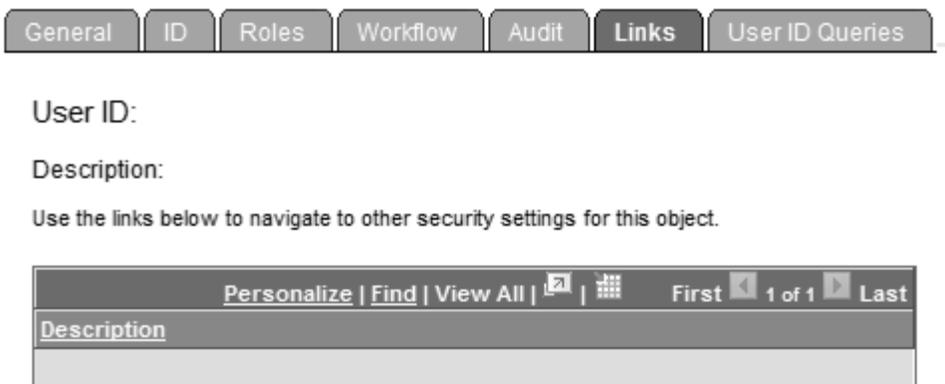


Figure 20: User Profiles Page - Links Tab

22. Complete the fields as follows:

User ID	Populated based on the user ID entered on the search/add criteria.
----------------	--

Description Populated based on the description entered on the search/add criteria.
Description Populated based on the description entered on the search/add criteria.

23. Select the **User ID Queries** tab. The User Profiles page - User ID Queries tab is displayed.

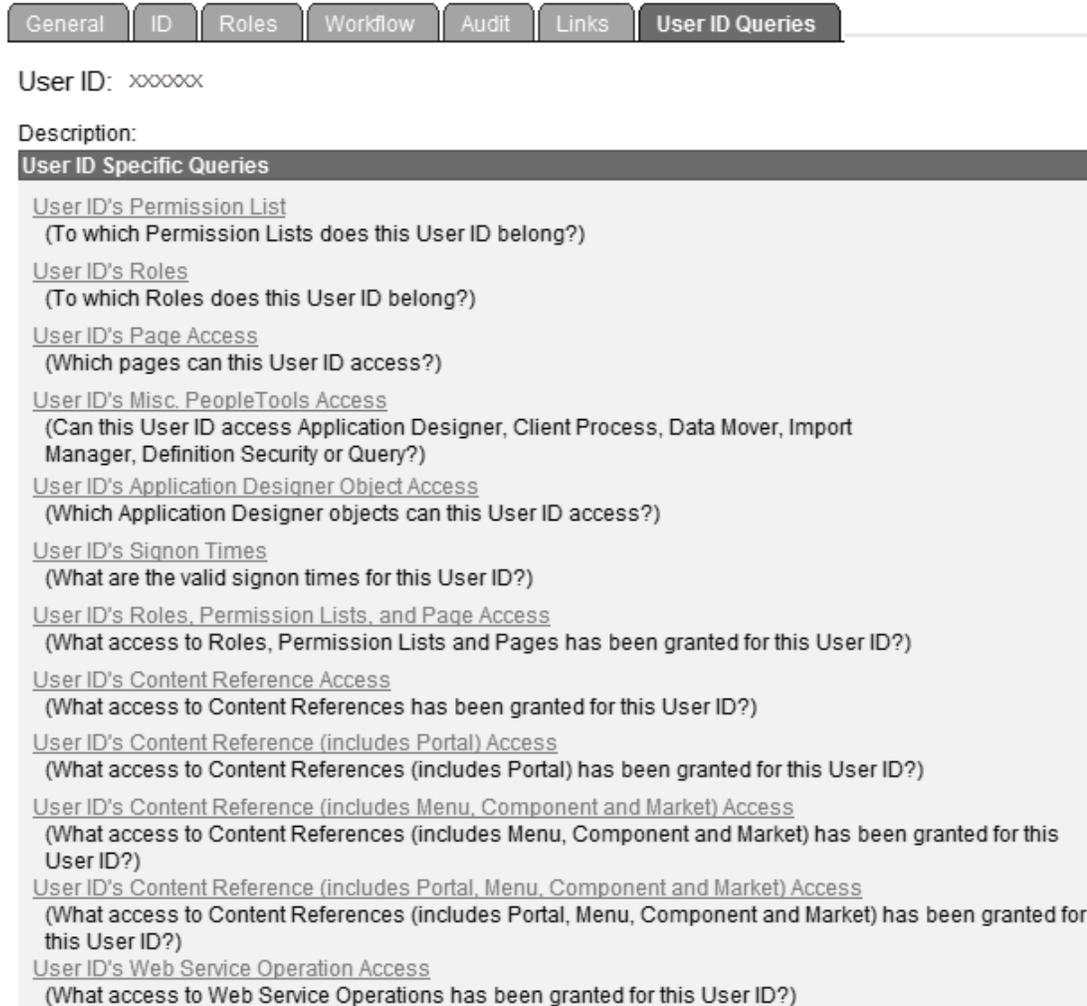


Figure 21: User Profiles Page - User ID Queries Tab

24. Complete the fields as follows:

User ID Populated based on the user ID.
Description Populated based on the description entered on the search/add criteria.
User ID Specific Queries Displays a list of the following links:

- **User ID's Permission List.** This link includes: To which Permission Lists does this User ID belong?
- **User ID's Roles.** This link includes: To which Roles does this User ID belong?

- **User ID's Page Access.** This link includes: Which pages can this User ID access?
- **User ID's Misc. PeopleTools Access.** This link includes: Can this User ID access Application Designer, Client Process, Data Mover, Import Manager, Definition Security or Query?
- **User ID's Application Designer Object Access.** This link includes: Which Application Designer objects can this User ID access?
- **User ID's Signon Times.** This link includes: What are the valid signon times for this User ID?
- **User ID's Roles, Permission Lists, and Page Access.** This link includes: What access to Roles, Permission Lists and Pages has been granted for this User ID?
- **User ID's Content Reference Access.** This link includes: What access to Content References has been granted for this User ID?
- **User ID's Content Reference (includes Portal) Access.** This link includes: What access to Content References (includes Portal) has been granted for this User ID?
- **User ID's Content Reference (includes Menu, Component and Market) Access.** This link includes: What access to Content References (includes Menu, Component and Market) has been granted for this User ID?
- **User ID's Content Reference (includes Portal, Menu, Component and Market) Access.** This link includes: What access to Content References (includes Portal, Menu, Component and Market) has been granted for this User ID?
- **User ID's Web Service Operation Access.** This link includes: What access to Web Service Operations has been granted for this User ID?

1. Click **Save** to save the information. At this point, the following options are available:

Step	Description
Click Add	Returns to the Add a New Value tab.
Click Update/Display	Returns to the Find an Existing Value tab.

Copy User Profiles

The **Copy User Profiles** option is used to copy a user profile.

To copy a user profile:

1. Select the **People Tools** menu group.
2. Select the **User Profiles** menu.

3. Select the **Copy User Profiles** component. The Copy User Profiles page - Find an Existing Value tab is displayed.

Copy User Profiles

Enter any information you have and click Search. Leave fields blank for a list of all values.



Figure 22: Copy User Profiles Page - Find an Existing Value Tab

4. Enter the applicable search criteria.
5. Click **Search**. The Copy User Profiles page is displayed.

Copy User Profiles

Existing User ID: xxxxxx

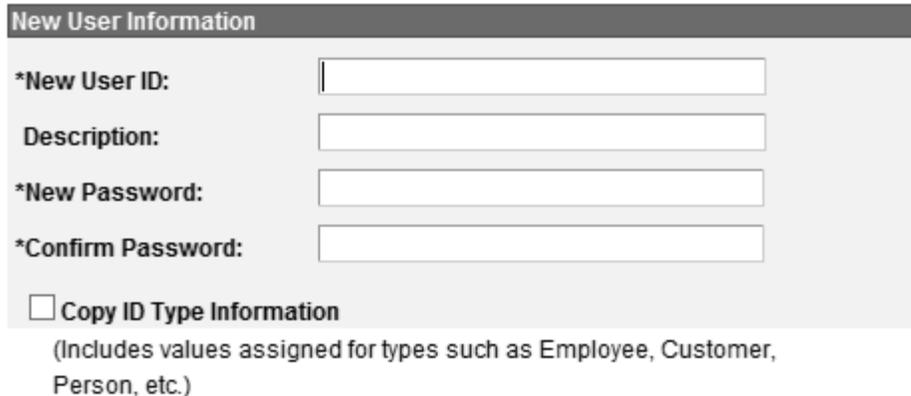


Figure 23: Copy User Profiles Page

6. Complete the fields as follows:

Existing User ID Populated.

New User Information

***New User ID** Enter the new user ID.

Description Enter the description of the new user ID.

- *New Password** Enter the new password for the new user ID.
- *Confirm Password** Reenter the new password for the new user ID.
- Copy ID Type Information** Check this box to include values assigned for types such as Employee, Customer, Person, etc.

7. Click **Save** to save the information. The User Profiles page - General tab is displayed. At this point, the following options are available:

Step	Description
Click Return to Search	Displays the Copy User Profiles page - Find an Existing Value tab.
Click Refresh	Refreshes the page.

Delete User Profiles

The **Delete Users Profile** option is used to delete a user profile.

To delete a user profile:

1. Select the **People Tools** menu group.
2. Select **Security**.
3. Select the **User Profiles** menu.
4. Select the **Delete User Profiles** component. The Delete User Profile page - Find an Existing Value tab is displayed.

Delete User Profile

Enter any information you have and click Search. Leave fields blank for a list of all values.



The screenshot shows a search interface with a 'Find an Existing Value' button, a 'Search Criteria' dropdown menu, and a 'Search by:' section. The 'Search by:' section includes a dropdown menu set to 'User ID', a 'begins with' label, and an empty text input field. Below this is a 'Case Sensitive' checkbox which is currently unchecked.

Figure 24: Delete User Profile Page - Find an Existing Value Tab

5. Enter the applicable search criteria.

6. Click **Search**. The Delete User Profile page is displayed.

Delete User Profile

User ID: xxxxx

Name:

Empl ID: xxxxxxx

Delete User Profile

Figure 25: Delete User Profile Page

7. Complete the fields as follows:

User ID	Populated based on the search/add criteria.
Name	Populated with the corresponding search/add criteria entered.
EmplID	Populated with the corresponding search/add criteria entered.

8. Click **Delete User Profile**. The User Profile Delete Confirmation popup appears.

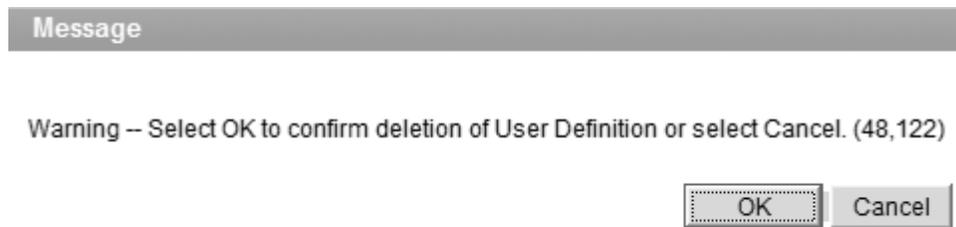


Figure 26: User Profile Delete Confirmation Popup

9. Click **OK** to delete the permissions list and return to the Delete User Profile page - Find an Existing Value tab.

OR

Click **Cancel** to cancel the deletion and return to the Delete User Profile page - Find an Existing Value tab.

Distributed User Profiles

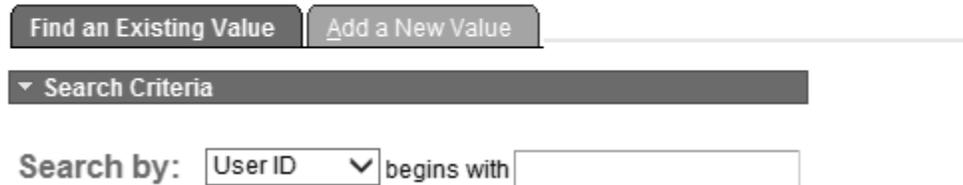
This option allows the user to create and maintain user profiles.

1. Select the **People Tools** menu group.

2. Select the **User Profiles** menu.
3. Select the **Distributed User Profiles** component. The Distributed User Profile page - Find an Existing Value tab is displayed.

Distributed User Profile

Enter any information you have and click Search. Leave fields blank for a list of all values.



The screenshot shows the 'Find an Existing Value' tab selected. Below the tabs is a 'Search Criteria' dropdown menu. Underneath, the 'Search by:' section has a dropdown menu set to 'User ID' and a text input field labeled 'begins with'.

Figure 27: Distributed User Profile Page - Find an Existing Value Tab

4. Enter the applicable search criteria.
5. Click **Search**. The User Profile page - General tab is displayed.

OR

Select the **Add a New Value** tab. The Distributed User Profile page - Add a New Value tab is displayed.

Distributed User Profile



The screenshot shows the 'Add a New Value' tab selected. Below the tabs is a 'User ID:' label followed by a text input field.

Figure 28: Distributed User Profile Page - Add a New Value Tab

6. Complete the User ID field as follows:

User ID Enter the user ID to be added. Spaces are not allowed when typing the user ID. Spaces will result in an error message.

7. Click **Add**. The User Profile page - General tab is displayed. For more information, refer to the **User Profiles** section of this procedure manual.

Distributed User Set Up

This option allows the user to set up the distributed user profile component search record.

1. Select the **People Tools** menu group.
2. Select the **User Profiles** menu.
3. Select the **Distributed User Set Up** component. The Set Distributed User Profile Search Record page is displayed.

Set Distributed User Profile Search Record

Current Search Record: Z_PSOPRDEFN_SRC

New Search Record: 

Figure 29: Set Distributed User Profile Search Record Page

4. Complete the fields as follows:

Current Search Record Populated based upon the current user's session.

New Search Record Enter the new search record or select data by clicking the search icon.

5. Click **Save** to save the new search record.

Purge Inactive User Profiles

This option allows the user to remove user profiles that have not been used for a long period of time.

1. Select the **People Tools** menu group.
2. Select the **User Profiles** menu.

3. Select the **Purge Inactive User Profiles** component. The Purge Inactive User Profiles page - Find an Existing Value tab is displayed.

Purge Inactive User Profiles

Enter any information you have and click Search. Leave fields blank for a list of all values.

Figure 30: Purge Inactive User Profiles Page - Find an Existing Value Tab

4. Complete the fields as follows:

Search by: Run Control ID begins with Enter the run control ID.

Case Sensitive Check this box if the run control ID is case sensitive.

5. Click **Search**. The Purge Inactive User Profiles page is displayed.

OR

Select the **Add a New Value** tab. The Purge Inactive User Profiles page - Add a New Value tab is displayed.

Purge Inactive User Profiles

Figure 31: Purge Inactive User Profiles Page - Add a New Value Tab

6. Complete the field as follows:

Run Control ID Enter the run control ID to be added. Spaces are not allowed when typing

the user ID. Spaces will result in an error message.

7. Click **Add**. The Purge Inactive User Profiles page is displayed. For more information, refer to the **User Profiles** section of this procedure.

Purge Inactive User Profiles

Purge the system of user profiles that have not been used in a specified amount of time. This aids in general housekeeping.

Go to: [Setup Purge Frequency for Inactive User Profiles](#)

Run Control ID:	test	Report Manager	Process Monitor	<input type="button" value="Run"/>
-----------------	------	--------------------------------	---------------------------------	------------------------------------

Figure 32: Purge Inactive User Profiles Page

8. Click the **Setup Purge Frequency for Inactive User Profiles** link. The Password Controls page is displayed. For more information about password controls, refer to the **Password Controls** section of this procedure.

Permissions and Roles

For more information see:

Permission Lists	31
Copy Permission Lists	57
Delete Permission Lists	59
Roles Component	60
Copy Roles	70
Delete Roles	71
Execute Role Rules.....	73

Permission Lists

Permission lists are groups of authorizations that are assigned to roles. A permission list may contain one or more types of permissions. The fewer types of permission in the permission list the more modular and scalable an implementation. The granularity of the permission lists is dependant upon the organizational needs.

Permission lists include the following:

- Sign-on times

- Page access
- PeopleTools access

A user profile inherits most of its permissions through the roles that have been assigned to the user profile. Some permission lists, such as process profile or row-level security, are applied directly to a user profile. Data permission, or row-level security, displays either through a primary list or a row-security permission lists.

To add a new permission list to a role, add more rows. Remember that a user’s access is determined by the sum of all the permission lists applied to each role to which the user belongs.

To create, maintain, copy, and delete permission lists:

1. Select the *EmpowHR User Security (HD)* menu group.
2. Select **Permission Lists**. The Permission Lists page - Find an Existing Value tab is displayed.

Permission Lists

Enter any information you have and click Search. Leave fields blank for a list of all values.



Figure 33: Permission Lists Page - Find an Existing Value Tab

3. Enter the applicable search criteria.
4. Click **Search**. The Permissions List page - General tab is displayed.

OR

Select the **Add a New Value** tab. The Permission Lists page - Add a New Value tab is displayed.

Permission Lists



Find an Existing Value **Add a New Value**

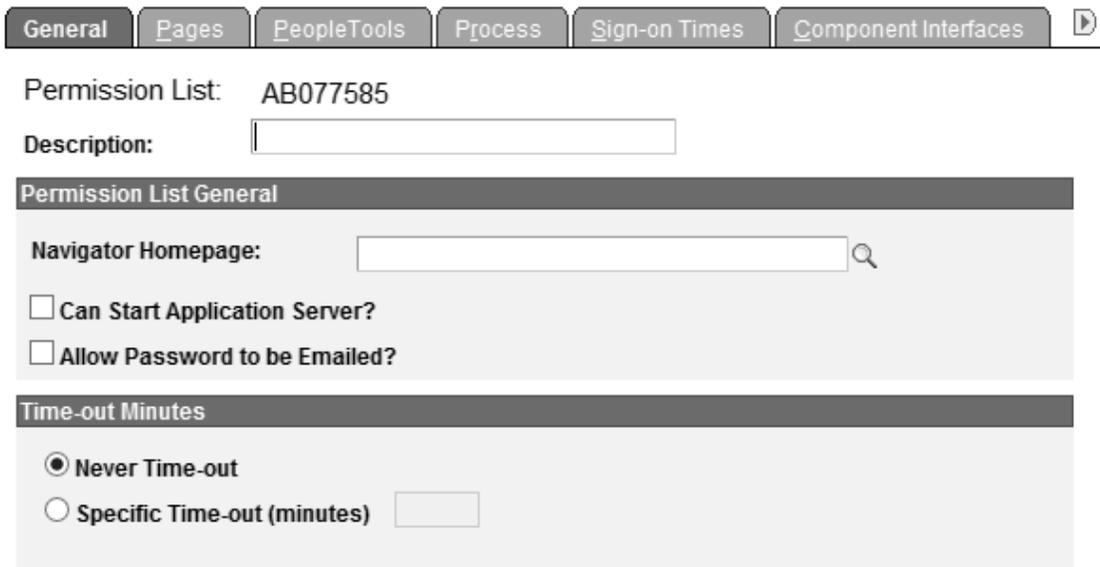
Permission List:

Figure 34: Permission Lists Page - Add a New Value Tab

5. Complete the field as follows:

Permission List Enter the applicable information.

6. Click **Add**. The Permissions Lists page - General tab is displayed. This tab sets general or miscellaneous attributes and system defaults.



General Pages PeopleTools Process Sign-on Times Component Interfaces

Permission List: AB077585

Description:

Permission List General

Navigator Homepage: 

Can Start Application Server?

Allow Password to be Emailed?

Time-out Minutes

Never Time-out

Specific Time-out (minutes)

Figure 35: Permission Lists Page - General Tab

7. Complete the fields as follows:

Permission List Populated based on the search criteria entered.

Description Enter the description of the Permission List. The information entered in this field will populate the Description field on subsequent tabs. If this field is left blank, the Description field will be blank on subsequent tabs.

Permission List General

Navigator Homepage Enter the applicable Navigator Homepage or select data by clicking the search icon.

Can Start Application Server? Check this box if applicable.

Allow Password to be Emailed? Check this box if applicable.

Time-out Minutes

Never Time-out Defaults to selected. Deselect if applicable.

Specific Time-out (minutes) Enter a value to represent the number of minutes before the application will time out in the second part of the field.

8. Select the **Pages** tab. The Permission Lists page - Pages tab is displayed. This tab sets page permissions.



The screenshot shows a web interface with a navigation bar containing tabs: General, Pages (selected), PeopleTools, Process, Sign-on Times, and Component Interfaces. Below the tabs, the text reads "Permission List: AB077585" and "Description:". A section titled "Mobile Page Permissions" is visible. Below this is a table with the following structure:

Menus		Personalize	Find	View All	First	1 of 1	Last
Menu Name	Menu Label	Edit Components					
<input type="text"/>		Edit Components		+	-		

Figure 36: Permission Lists Page - Pages Tab

9. Complete the fields as follows:

Permission List Populated based on the search criteria entered.

Description Populated based on the description entered on the Permission Lists page - General tab.

Menus

Menu Name Enter the applicable menu name or select data by clicking the search icon.

Menu Label Populated based on the menu name entered.

Edit Components Populated.

10. Click the **Mobile Page Permissions** link. The Mobile Page Permissions page is displayed.

Mobile Page Permissions

Permission List: AB077585

Description:

Mobile Pages		Personalize	Find	View All	First	1 of 1	Last
Mobile Page Name	Description						
<input type="text"/>							

Figure 37: Mobile Page Permissions Page

11. Complete the fields as follows:

- Permission List** Populated based on the search criteria entered.
- Description** Populated based on the description entered on the Permissions page - General tab.
- Mobile Pages**
- Mobile Page Name** Enter the mobile page name or select data by clicking the search icon.
- Description** Populated based upon the Mobile Page Name entered.

12. Click **OK**. The information is saved. The Permission Lists page - Pages tab is displayed.

OR

Click **Cancel**. The Permission Lists page - Pages tab is displayed.

13. Click the **Edit Components** link. The Component Permissions page is displayed.

Component Permissions

Administer FMLA

Components					Personalize	Find	First	1-3 of 3	Last
Authorized?	Component Name	Item Label	Edit Pages	View Content References for this Component					
<input type="checkbox"/>	FMLA_LEAVE_ADMIN	Request/Authorize/Track Leave	Edit Pages	View					
<input type="checkbox"/>	RUN_BEN020	Status Report	Edit Pages	View					
<input type="checkbox"/>	RUN_BEN021	Payroll Audit Report	Edit Pages	View					

Figure 38: Component Permissions Page

14. Complete the fields as follows:

Components

Authorized?	Check this box if applicable.
Component Name	Displays the component to be select.
Item Label	Describes the Component Name.
Edit Pages	Click to edit the information.
View Content References for this Component	Click to view the component.

15. Click **Select All** to select all available components.

OR

Click **Deselect All** to deselect all components.

16. Click **OK**. The information is saved and the Component Permissions page is displayed.

OR

Click **Cancel**. The Component Permissions page is displayed.

17. Click the **Edit** link, if applicable. The Content References page is displayed. This page displays all the content references in the database that point to this component. If the Accessible column is checked, the Permission List is displayed. This Permission List includes access to all parent folders of the content reference.

18. Click **Return**. The Component Permissions pages is displayed.

19. Click **OK** to save the information. The Permission Lists page - Pages tab is displayed.

OR

Click **Cancel** to cancel the action. The Permission Lists page - Pages tab is displayed.



Figure 39: Permission Lists Page - Pages Tab

20. Select the **People Tools** tab. The Permission Lists page - PeopleTools tab is displayed. This tab grants access to the PeopleTools application and grants access for specific options within PeopleTools.

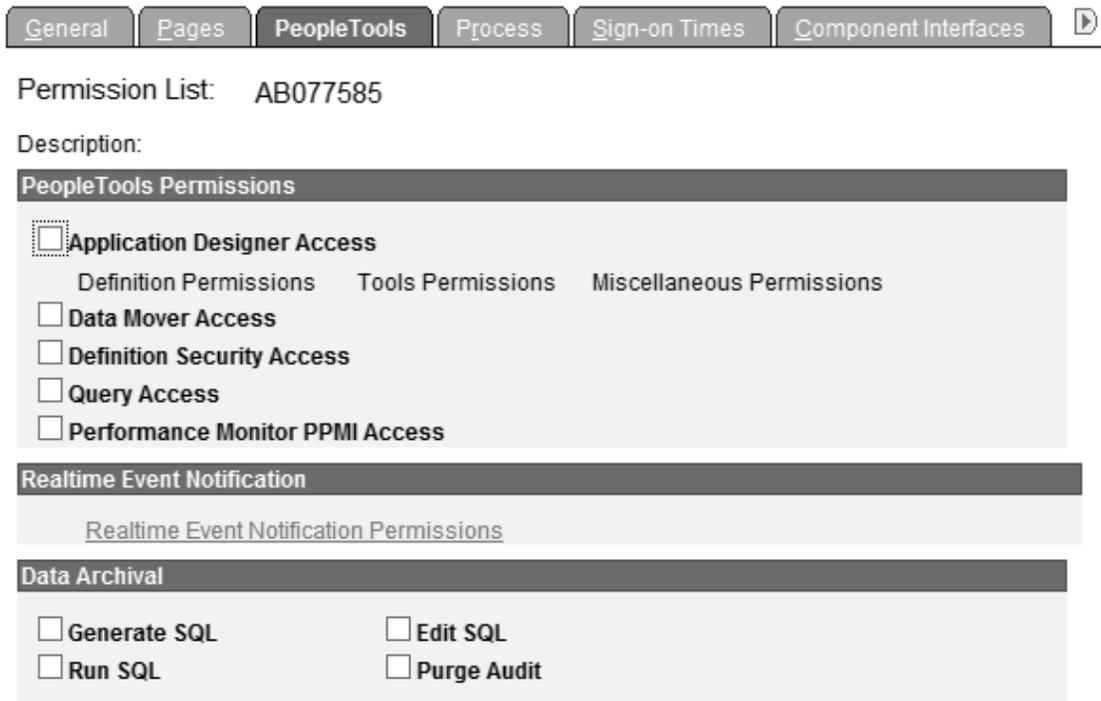


Figure 40: Permission Lists Page - PeopleTools Tab

21. Complete the fields as follows:

Permission List Populated based on the search criteria entered.

Description	Populated based on the description entered on the Permission Lists page - General tab.
PeopleTools Permissions	
Application Designer Access	Check this box to activate the Definition Permissions , Tools Permissions , and Miscellaneous Permissions links. These links allow a user to define various permissions in the application.
Data Mover Access	Check this box to activate data mover access.
Definition Security Access	Check this box to activate definition security access.
Query Access	Check this box to activate query access.
Performance Monitor PPMI Access	Check this box to activate performance monitor Performance Monitor Integration (PPMI) access.
Realtime Event Notification	
Data Archival	
Generate SQL	Check this box to allow users to generate an SQL.
Edit SQL	Check this box to allow users to edit an SQL.
Run SQL	Check this box to allow users to run an SQL.
Purge Audit	Check this box to allow users to purge an audit.

22. Click the **Definition Permissions** link. The Definition Permissions page is displayed.

Definition Permissions

Permission List: AB077585

Description:

Object	*Access
Activity	No access
Analytic Model	No access
App Engine Program	No access
Application Package	No access
Approval Rule Set	No access
Business Interlink	No access
Business Process	No access
Component	No access
Component Interface	No access
Field	No access
File Layout	No access
File Reference	No access
HTML	No access
Image	No access
Menu	No access
Merge	No Access
Message	No access
Message Channel	No access
Message Node	No access
Mobile Pages	No access
Optimization Model	No access
Page	No access
PeopleCode Work-In-Progress	No Access
Problem Type	No access
Project	Full access
Record	No access
Style Sheet	No access
Type Code	No access
Visual Merge Page	No Access

Full Access (All)
 Read Only (All)
 No Access (All)

Figure 41: Definition Permissions Page

23. Complete the fields as follows:

Permission List	Populated based on the search criteria entered.
Description	Populated based on the description entered on the Permission List page - General tab.
Object	Populated.
*Access	Select data from the drop-down list. Valid values are Full Access , Read Only Access , and No Access .

At this point, the following options are available:

Step	Description
Click Full Access (All)	Applies to all objects.
Click Read Only (All)	Applies read only to all objects.
Click No Access (All)	Applies no access to all objects.

24. Click **OK** to save the data. The Permission Lists page - People Tools tab is displayed.

OR

Click **Cancel** to cancel the action. The Permission Lists page - People Tools tab is displayed.

25. Click the **Tools Permissions** link. The Tools Permission page is displayed. The access code drop-down list for each tool listed may vary depending on the permission list selected.

Tools Permission

Permission List: AB077585

Description:

Tool	*Access Code
Build / Data Admin.	No access
Change Control	Supervisor ac
Language Translations	No access
Peoplecode Debugger	No access
SQL Editor	No access
Upgrade	No access

Full Access (All)
Read Only (All)
No Access (All)

Figure 42: Tools Permission Page

26. Complete the fields as follows:

Permission List	Populated based on the search criteria entered.
Description	Populated based on the description entered on the Permission Lists page - General tab.
Tool	Populated.
*Access Code	Enter the applicable information or select data from the drop-down list. The access code drop-down list for each tool listed may vary depending on the permission list selected.

At this point, the following options are available:

Step	Description
Click Full Access (All)	Applies to all objects.
Click Read Only (All)	Applies read only to all objects.
Click No Access (All)	Applies no access to all objects.

27. Click **OK** to save the data. The Permission Lists page - PeopleTools tab is displayed.

OR

Click **Cancel** to cancel the action. The Permission Lists page - PeopleTools tab is displayed.

28. Click the **Miscellaneous Permissions** link. The Miscellaneous Permissions page is displayed.

Miscellaneous Permissions

Permission List: AB077585

Description:

Feature	*Access
Access Profiles	No access
Color	No access
Field Format	No access
Style	No access
Tool Bar	No access

Full Access (All)
 Read Only (All)
 No Access (All)

Figure 43: Miscellaneous Permissions Page

29. Complete the fields as follows:

Permission List	Populated based on the search criteria entered.
Description	Populated based on the description entered on the Permission Lists page - General tab.
Feature	Populated.
*Access	Enter the applicable information or select data from the drop-down list. Valid values are Full Access , Read Only Access , and No Access .

At this point, the following options are available:

Step	Description
Click Full Access (All)	Applies to all objects.
Click Read Only (All)	Applies read only to all objects.
Click No Access (All)	Applies no access to all objects.

30. Click **OK** to save the data. The Permission Lists page - PeopleTools tab is displayed.

OR

Click **Cancel** to cancel the action. The Permission Lists page - PeopleTools tab is displayed.

31. Click the **Realtime Event Notification Permissions** link. The REN Permissions page is displayed.

REN Permissions

Permission List: AB077585

Description:

Object	*Access Code
MCF Agent	No Access
MCF CTI Server	No Access
MCF Customer	No Access
MCF MCFLOG Server	No Access
MCF Notify Queue	No Access
MCF Supervisor	No Access
MCF UQSRV Server	No Access
Optimization Notify	No Access
Reporting Window	No Access

Buttons: Full Access (All), No Access (All), OK, Cancel

Figure 44: REN Permissions Page

32. Complete the fields as follows:

Permission List	Populated based on the search criteria entered.
Description	Populated based on the description entered on the Permission List page - General tab.
Object	Populated.
*Access Code	Enter the applicable information or select data from the drop-down list. Valid values are Full Access and No Access .

At this point, the following options are available:

Step	Description
Click Full Access (All)	Applies to all objects.
Click Read Only (All)	Applies read only to all objects.
Click No Access (All)	Applies no access to all objects.

33. Click **OK** to save the data. The Permission Lists page - PeopleTools tab is displayed.

OR

Click **Cancel** to cancel the action. The Permission Lists page - PeopleTools tab is displayed.

34. Select the **Process** tab. The Permission Lists page - Process tab is displayed. This tab specifies to what capacity a user or role can modify *EmpowHR* Process Scheduler settings.

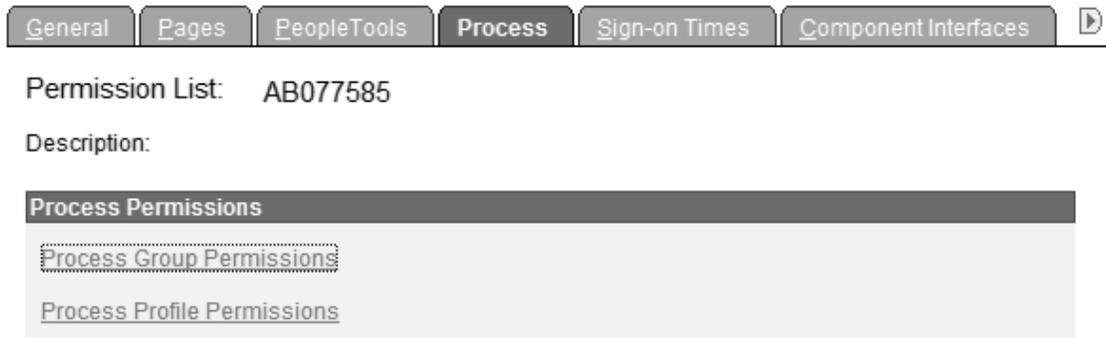


Figure 45: Permission Lists Page - Process Tab

35. Complete the fields as follows:

Permission List	Populated based on the search criteria entered.
Description	Populated based on the description entered on the Permission Lists page - General tab.
Process Permissions	
Process Group Permissions	Links to the Process Group Permission page.
Process Profile Permissions	Links to the Process Profile Permissions page.

36. Click the **Process Group Permissions** link. The Process Group Permission page is displayed.

Process Group Permission

Permission List: AB077585

Description:

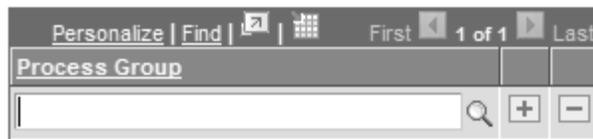


Figure 46: Process Group Permission Page

37. Complete the fields as follows:

- | | |
|------------------------|--|
| Permission List | Populated based on the search criteria entered. |
| Description | Populated based on the description entered on the Permission Lists page - General tab. |
| Process Group | Enter the process group or select data by clicking the search icon. |

38. Click **OK** to save the data. The Permission Lists page - Process tab is displayed.

OR

Click **Cancel** to cancel the action. The Permission Lists page - Process tab is displayed.

39. Click the **Process Profile Permissions** link. The Process Profile Permission page is displayed.

Process Profile Permission

Permission List: AB077585

Description:

Server Destinations	Allow Requestor To
File: <input type="text"/>	<input type="checkbox"/> Override Output Destination
Printer: <input type="text"/>	<input type="checkbox"/> Override Server Parameters
OS/390 Job Controls	
Name: <input type="text"/>	<input type="checkbox"/> View Server Status
Acct: <input type="text"/>	<input type="checkbox"/> Update Server Status
Allow Process Request	
*View By: <input type="text" value="None"/> ▼	<input type="checkbox"/> Enable Recurrence Selection
*Update By: <input type="text" value="None"/> ▼	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Figure 47: Process Profile Permission Page

40. Complete the fields as follows:

Permission List	Populated based on the search criteria entered.
Description	Populated based on the description entered on the Permission Lists page - General tab.
Server Destinations	
File	Enter the applicable file name for the server destination.
Printer	Enter the applicable printer name for the server destination.
Allow Requestor To	
Override Output Destination	Check this box if applicable.
Override Server Parameters	Check this box if applicable.
View Server Status	Check this box if applicable.

- Update Server Status** Check this box if applicable.
- Enable Recurrence Selection** Check this box if applicable.
- OS/390 Job Controls**
- Name** Enter the name for the job controls.
- Acct** Enter the account for the job controls.
- Allow Process Request**
- *View By** Select the applicable information from the drop-down list. Valid values are **All**, **None**, and **Owner**.
- *Update By** Select the applicable information from the drop-down list. Valid values are **All**, **None**, and **Owner**.

41. Click **OK** to save the data. The Permission Lists page - Process tab is displayed.

OR

Click **Cancel** to cancel the action. The Permission Lists page - Process tab is displayed.

42. Select the **Sign-on Times** tab. The Permission Lists page - Sign-on Times tab is displayed. This tab specifies when users are authorized to sign in to *EmpowHR*. If users are signed in to the application when the sign-in time expires, they are automatically signed out.

Permission List: AB077585

Description:

*Day	Start	Time	End	Time		
Sunday	00	00	23	59	+	-
Monday	00	00	23	59	+	-
Tuesday	00	00	23	59	+	-
Wednesday	00	00	23	59	+	-
Thursday	00	00	23	59	+	-
Friday	00	00	23	59	+	-
Saturday	00	00	23	59	+	-

Figure 48: Permission Lists Page - Sign-on Times Tab

43. Complete the fields as follows:

Permission List	Populated based on the search criteria entered.
Description	Populated based on the description entered on the Permission Lists page - General tab.
Sign-on Times	
*Day	Select the applicable day from the drop-down list.
Start	Enter the applicable hour for the start time.
Time	Enter the applicable minute(s) for the start time.
End	Enter the applicable hour for the end time.
Time	Enter the applicable minute(s) for the end time.

44. Select the **Component Interfaces** tab. The Permission Lists page - Component Interfaces tab is displayed. This tab grants access to any component interfaces that a user may need to use to complete a transaction.



Figure 49: Permission Lists Page - Component Interfaces Tab

45. Complete the fields as follows:

Permission List	Populated based on the search criteria entered.
Description	Populated based on the description entered on the Permission Lists page - General tab.
Component Interfaces	
Name	Enter the component interface name or select data by clicking the search icon.

46. Click the **Edit** link to edit the permissions for the component interface selected. The Component Interface Permissions page is displayed.

Component Interface Permissions

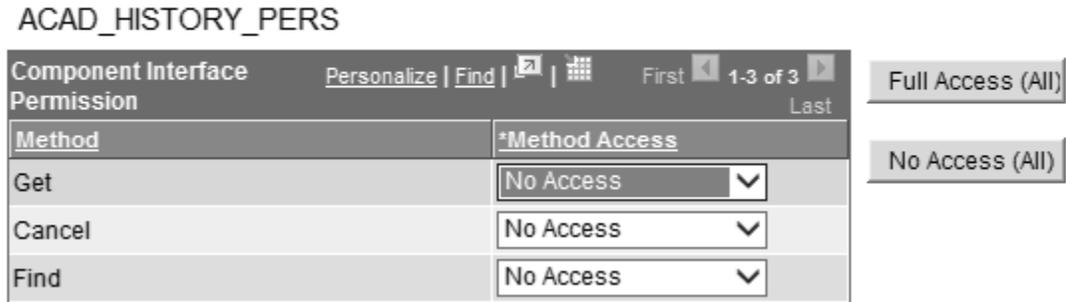


Figure 50: Component Interface Permissions Page

47. Complete the fields as follows:

Component Interface Permission

Method Populated.

***Method Access** Select the applicable access level from the drop-down list. Valid values are **Full Access** and **No Access**.

At this point, the following options are available:

Step	Description
Click Full Access (All)	Applies to all objects.
Click No Access (All)	Applies no access to all objects.

48. Click **OK** to save the data. The Permission Lists page - Component Interfaces tab is displayed.

OR

Click **Cancel** to cancel the action. The Permission Lists page - Component Interfaces tab is displayed.

49. Select the **Web Libraries** tab. The Permission Lists page - Web Libraries tab is displayed. This tab sets Web library permissions. Security Administrators should make sure that users have the proper access to Web libraries. If users do not have proper authorization to the Web library and its associated scripts, then they will not have proper access to the application. If users are not authorized for a particularity Web library or script, they cannot invoke it.

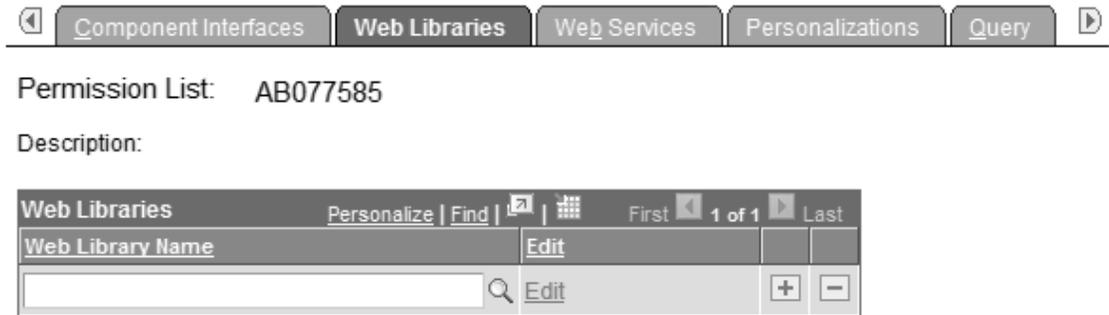


Figure 51: Permission Lists Page - Web Libraries Tab

50. Complete the fields as follows:

- Permission List** Populated based on the search criteria entered.
- Description** Populated based on the description entered on the Permissions Lists page - General tab.
- Web Libraries**
- Web Library Name** Enter the Web Library Name or select data by clicking the search icon. This file displays the Web libraries added to the permission list.

51. Click the **Edit** link. The Weblib Permissions page is displayed.

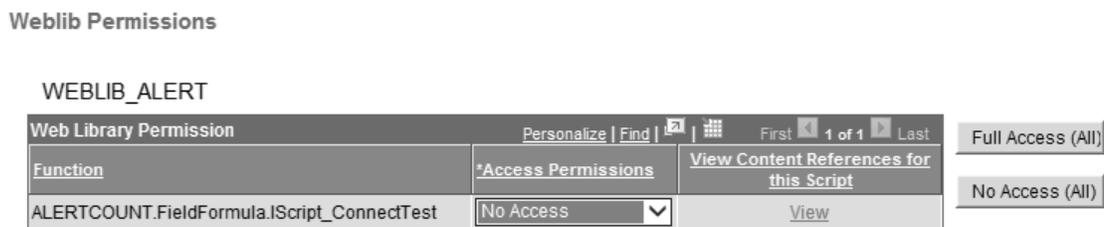


Figure 52: Weblib Permissions Page

52. Complete the fields as follows:

- Web Library Permission**
- Function** Populated.

***Access Permissions** Select the applicable permission level from the drop-down list. Valid values are **Full Access** and **No Access**.

At this point, the following options are available:

Step	Description
Click Full Access (All)	Applies to all objects.
Click No Access (All)	Applies no access to all objects.

Note: You can click the **View** link to display the Content References page. This page displays all the content references in this database that point to this script. If the Accessible column is checked, the Permission List is displayed. This Permission List includes access to all parent folders of the content reference.

53. Click **Return**. The Permission Lists page - Weblib Permissions tab is displayed.
54. Click **OK** to save the data. The Permission Lists page - Weblib Permissions tab is displayed.

OR

Click **Cancel** to cancel the action. The Permission Lists page Weblib - Permissions tab is displayed.

55. Select the **Personalizations** tab. The Permission Lists page - Personalizations tab is displayed. This tab sets which personalization users can use and which they can customize.

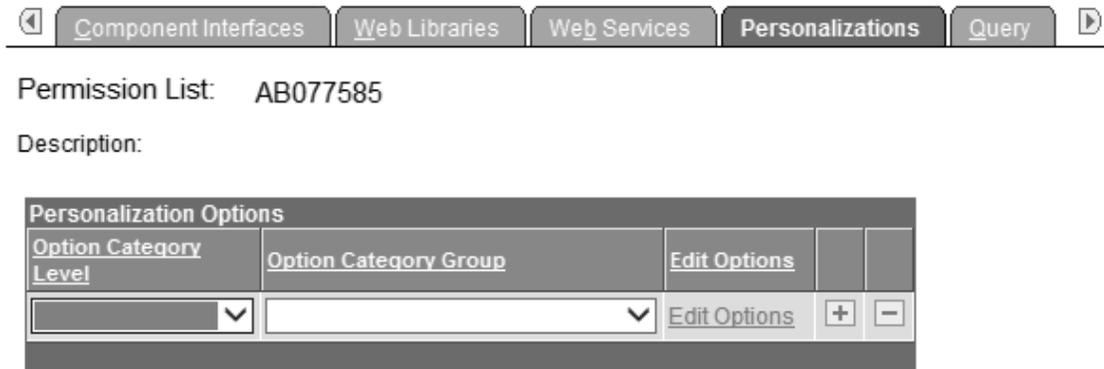


Figure 53: Permission Lists Page - Personalizations Tab

56. Complete the fields as follows:

Permission List Populated based on the search/add criteria entered.

Description Populated based on the description entered on the Permission Lists page - General tab.

Personalization Options

Option Category Level Select the applicable data from the drop-down list.

Option Category Group Select the applicable data from the drop-down list.

57. Click the **Edit Options** link. The Personalization Permissions page is displayed.

Personalization Permissions

Option Category Level:

Option Category Group:

Personalization Options			
Category	User Option	Description	Allow User Option
			<input checked="" type="checkbox"/>

Figure 54: Personalization Permissions Page

58. Complete the fields as follows:

Option Category Level Populated from the Permission Lists page - Personalizations tab.

Option Category Group Populated from the Permission Lists page - Personalizations tab.

Category Blank and cannot be modified.

User Option Blank and cannot be modified.

Description Blank and cannot be modified.

Allow User Option Check this box if the user is allowed to use the Personalization Options on the Permission Lists page - Personalizations tab.

At this point, the following options are available:

Step	Description
Click Select All	Selects all personalization options.
Click Deselect All	Deselects all personalization options.

59. Click **OK**. The data is saved and the Permission Lists page - Personalizations tab is displayed.

OR

Click **Cancel**. The action is canceled and the Permission Lists page - Personalizations tab is displayed.

60. Select the **Query** tab. The Permission Lists page - Query tab is displayed. This tab controls the query operations a user can perform and the data they can access while using *EmpowHR* Query.

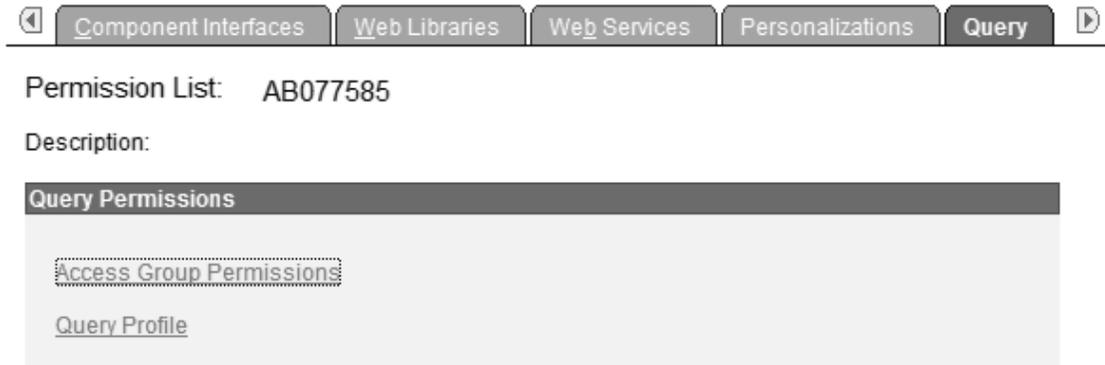


Figure 55: Permission Lists Page - Query Tab

61. Complete the fields as follows:

- Permission List** Populated based on the search criteria entered.
- Description** Populated based on the description entered on the Permission Lists page - General tab.
- Query Permissions**
- Access Group Permissions** Click this link to display the Permission List Access Groups page.
- Query Profile** Click this link to display the Query Profile page.

62. Click the **Access Group Permissions** link. The Permission List Access Groups page is displayed.

Permission List Access Groups

Permission List: AB077585
 Description:



Figure 56: Permission List Access Groups Page

63. Complete the fields as follows:

Permission List	Populated based on the search/add criteria entered.
Description	Populated based on the description entered on the Permission Lists page - General tab.
*Tree Name	Enter tree name or select data by clicking the search icon.
*Access Group	Enter access group or select data by clicking the search icon.
Accessible	Check this box if applicable.

64. Click **OK**. The data is saved and the The Permission List Access Groups page is displayed.

OR

Click **Cancel**. The action is canceled and the The Permission List Access Groups page is displayed.

65. Select the **Mass Change** tab. The Permission List page - Mass Change tab is displayed. This tab sets mass change security permissions.

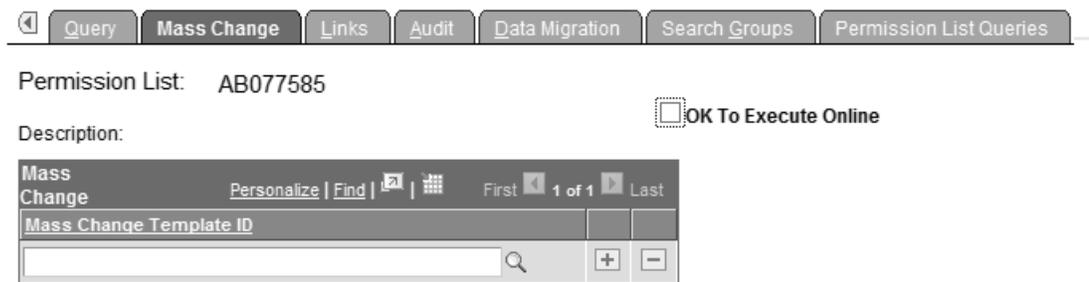


Figure 57: Permission Lists Page - Mass Change Tab

66. Complete the fields as follows:

Permission List	Populated based on the search/add criteria entered.
Description	Populated based on the description entered on the Permission Lists page - General tab.
OK To Execute Online	Check this box if applicable.
Mass Change	
Mass Change Template ID	Enter the Mass Change Template ID or select the applicable data by clicking the search icon.

67. Select the **Links** tab. The Permission Lists page - Links tab is displayed. The links tab is used to view links to other pages within *EmpowHR* that pertain to a particular permission list.

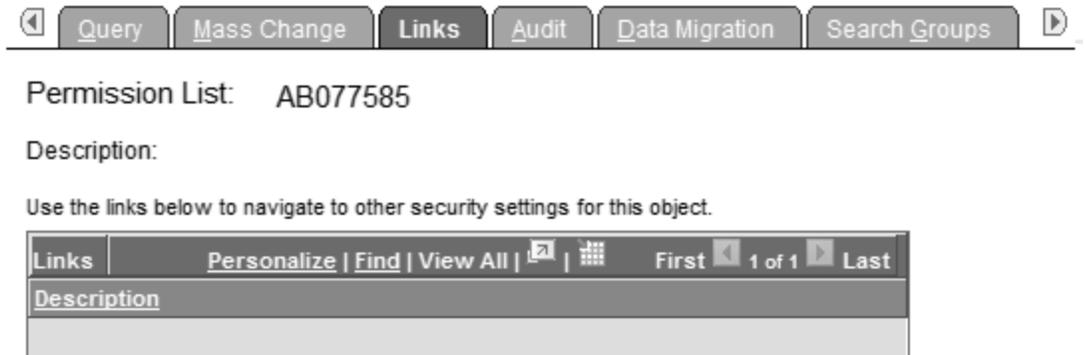


Figure 58: Permission Lists Page - Links Tab

68. Complete the fields as follows:

- Permission List** Populated based on the search/add criteria entered.
- Description** Populated based on the description entered on the Permission Lists page - General tab.
- Links**
 - Description** Click this link to sort by description.

69. Select the **Audit** tab. The Permission Lists page - Audit tab is displayed. This tab allows the user to inquire when a permission list was last updated and by whom.

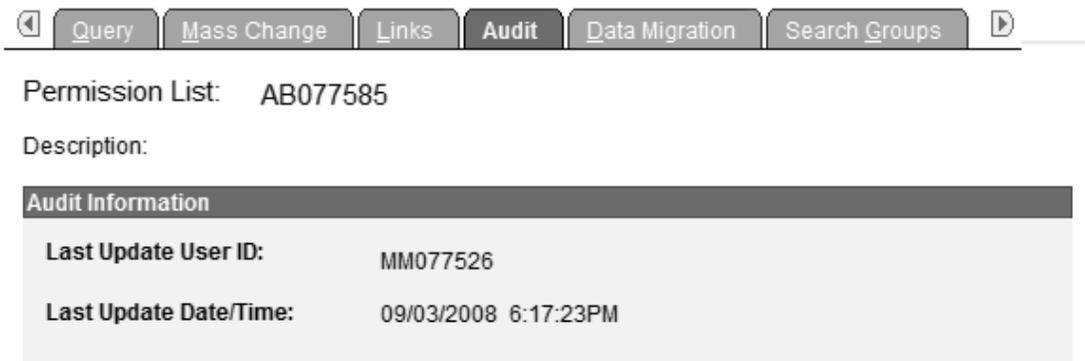


Figure 59: Permission Lists Page - Audit Tab

70. Complete the fields as follows:

- Permission List** Populated based on the search/add criteria entered.

Description	Populated based on the description entered on the Permission Lists page - General tab.
Audit Information	
Last Update User ID	Populated with the last update.
Last Update Date/Time	Populated with the last date/time the user ID was updated.

71. Select the **Permission List Queries** tab. The Permission Lists page - Permission List Queries tab is displayed.

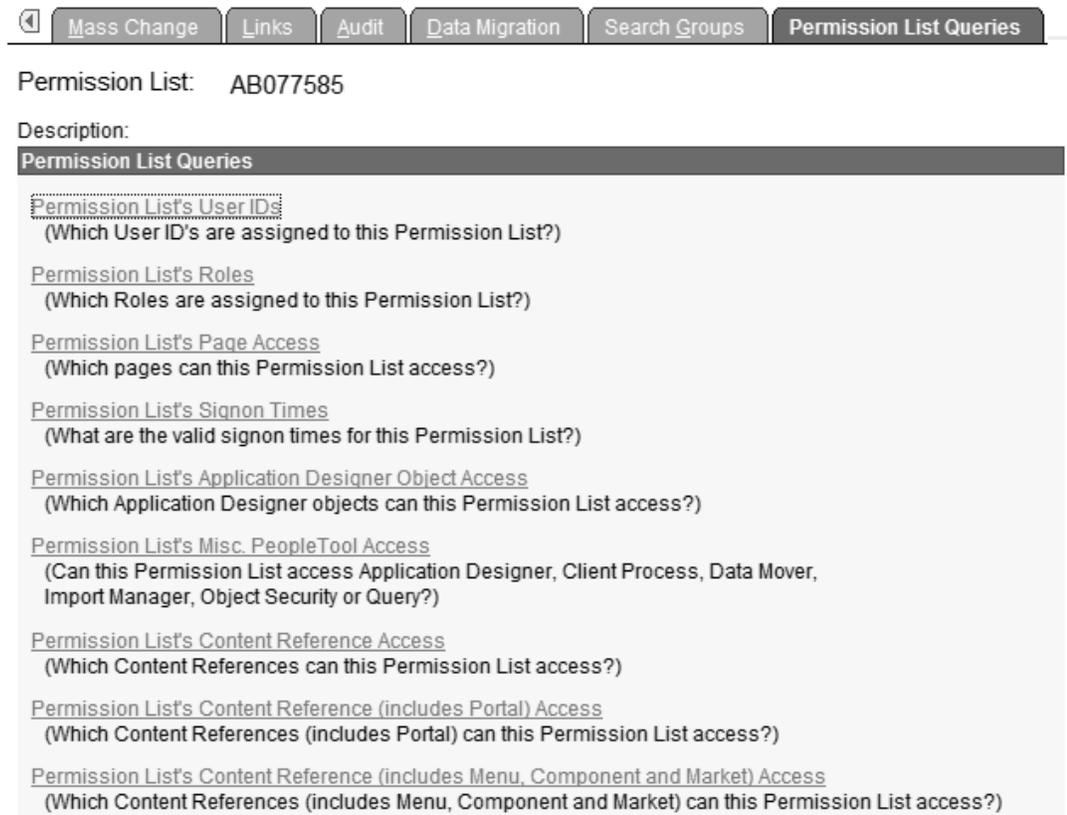


Figure 60: Permission Lists Page - Permission Lists Queries Tab

72. Complete the fields as follows:

Permission List	Populated based on the search criteria entered.
Description	Populated based on the description entered on the Permission Lists page - General tab.
Permission List Queries	Displays a list of links that allow the user to perform queries. Below is a list of the links as follows: <ul style="list-style-type: none"> • Permission List's User IDs. This link includes: Which User ID's are assigned to this Permission List? • Permission List's Roles. This link includes: Which Roles

- are assigned to this Permission List?
- **Permission List's Page Access.** This link includes: Which pages can this Permission List access?
 - **Permission List's Signon Times.** This link includes: What are the valid signon times for this Permission List?
 - **Permission List's Application Designer Object Access.** This link includes: Which Application Designer objects can this Permission List access?
 - **Permission List's Misc. PeopleTool Access.** This link includes: Can this Permission List access Application Designer, Client Process, Data Mover, Import Manager, Object Security or Query?
 - **Permission List's Content Reference Access.** This link includes: Which Content References can this Permission List access?
 - **Permission List's Content Reference (includes Portal) Access.** This link includes: Which Content References (includes Portal) can this Permission List access?
 - **Permission List's Content Reference (includes Menu, Component and Market) Access.** This link includes: Which Content References (includes Menu, Component and Market) can this Permission List access?

1. Click **Save** to save the information.

At this point, the following options are available:

Step	Description
Click Add	Returns to the Add a New Value tab.
Click Update/Display	Updates the page.

Copy Permission Lists

The **Copy Permission Lists** option is used to copy a permission list.

To copy a permission lists:

1. Select the **People Tools** menu group.
2. Select the **Security** menu.
3. Select the **Permissions & Roles** component.
4. Select the **Permission Lists** menu item.

5. Select the **Copy Permission Lists** component. The Permission List Save As page - Find an Existing Value tab is displayed.

Permission List Save As

Enter any information you have and click Search. Leave fields blank for a list of all values.

Find an Existing Value

▼ Search Criteria

Search by: begins with

Figure 61: Permission List Save As Page - Find an Existing Value Tab

6. Enter the applicable search criteria.
7. Click **Search**. A list of matches is displayed.
8. Select the applicable item on the list. The Permission List Save As page is displayed.

Permission List Save As

Save Permission List AB077585 To:

Figure 62: Permission List Save As Page

9. Complete the fields as follows:

Save Permission List Defaults to the item selected on the list of matches displayed after clicking **Search** on the Permission List Save As page - Find an Existing Value tab.

To Enter the applicable information.

10. Click **Save** to save the copied permission list. At this point, the following options are available:

Step	Description
Click Return to Search	Returns to the Permission List Save As page - Find an Existing Value tab.
Click Refresh	Refreshes the page.

Delete Permission Lists

The **Delete Permission Lists** option is used to delete a copied permission list that has been saved.

To delete a permission list:

1. Select the **People Tools** menu group.
2. Select the **Security** menu.
3. Select the **Permissions & Role Lists** menu item.
4. Select the **Delete Permission Lists** component. The Delete Permission List page - Find an Existing Value tab is displayed.

Delete Permission List

Enter any information you have and click Search. Leave fields blank for a list of all values.

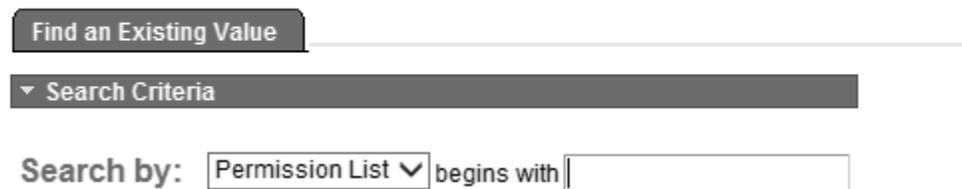


Figure 63: Delete Permission List Page - Find an Existing Value Tab

5. Enter the applicable search criteria.
6. Click **Search**. A list of matches is displayed.
7. Select the applicable item on the list. The Delete Permission List page is displayed.

Delete Permission List

Permission List Id: AB077585

Delete Permission List

Figure 64: Delete Permission List Page

8. Complete the field as follows:

Permission List ID Populated based on the item selected on the list of matches.

9. Click **Delete Permission List**. A Delete Permission Confirmation popup appears.



Figure 65: Delete Permission Confirmation Popup

10. Click **OK** to delete the permission list and return to the Delete Permission List page - Find an Existing Value tab.

OR

Click **Cancel** to cancel the deletion and return to the Delete Permission List page.

Roles Component

Roles are assigned to user profiles and are intermediate objects that link user profiles to permission lists. Multiple roles can be assigned to a user profile and multiple permission lists can be assigned to a role. Users are able to display both static and dynamic role member from two Roles pages.

- Roles - Members page
- Roles - Dynamic Members page

The Members page - Roles tab is used to display the current list of static role members. The Dynamic Members page - Roles tab is used to display the current list of dynamic roll members. If an Agency is not currently using the dynamic roles, then this list is not populated.

This option is used to create and maintain roles established in the database.

To create or modify a role:

The **Roles** option is used to create or modify a role.

1. Select the **People Tools** menu group.
2. Select the **Security** menu.
3. Select **Permissions & Roles**.

4. Select the **Roles** component. The Roles page - Find an Existing Value tab is displayed.

Roles

Enter any information you have and click Search. Leave fields blank for a list of all values.

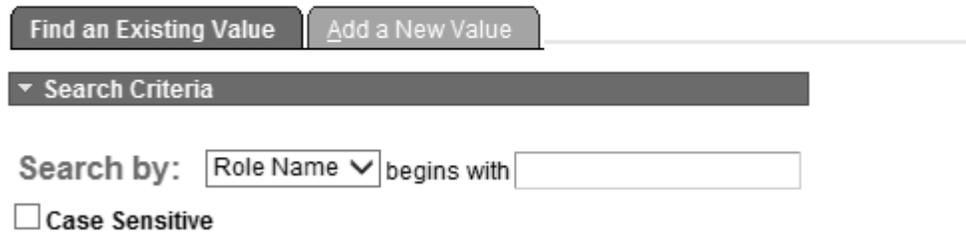


Figure 66: Roles Page - Find an Existing Value Tab

5. Enter the applicable search criteria.
6. Click **Search**. The Roles page - General tab is displayed.

OR

Select the **Add a New Value** tab. The Roles page - Add a New Value tab is displayed.

Roles

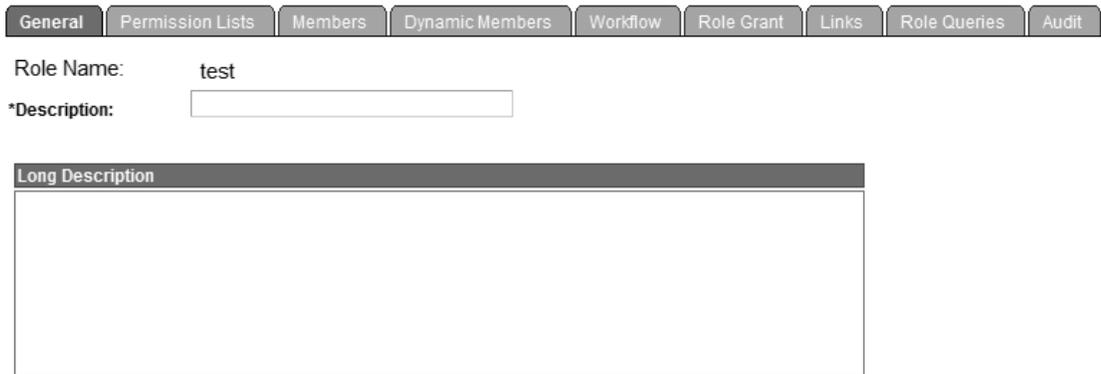


Figure 67: Roles Page - Add a New Value Tab

7. Complete the fields as follows:

Role Name Enter the role name.

8. Click **Add**. The Roles page - General tab is displayed.



The screenshot shows the 'Roles Page - General Tab' interface. At the top, there is a navigation bar with tabs: General, Permission Lists, Members, Dynamic Members, Workflow, Role Grant, Links, Role Queries, and Audit. Below the navigation bar, the 'Role Name' field is populated with 'test'. The '*Description' field is empty. Below the description field is a large text area labeled 'Long Description'.

Figure 68: Roles Page - General Tab

9. Complete the fields as follows:

Role Name Populated with the search/add criteria entered.

***Description** Enter the description of the role name.

Long Description Enter the long description of the role name.

10. Select the **Permission Lists** tab. The Roles page - Permission Lists tab is displayed.



The screenshot shows the 'Roles Page - Permission Lists Tab' interface. The navigation bar now has 'Permission Lists' selected. The 'Role Name' field is populated with 'test'. The 'Description' field is empty. Below the description field is a table with the following structure:

*Permission List	Description	View Definition
<input type="text"/>		View Definition

The table also includes a search icon in the first column and '+' and '-' icons in the third column. Above the table, there are controls for 'Personalize', 'Find', 'View All', and pagination for 'First 1 of 1 Last'.

Figure 69: Roles Page - Permission Lists Tab

11. Complete the fields as follows:

Role Name Populated with the search/add criteria entered.

Description Populated with the description of the role name.

Permission Lists

Permission List Enter the permission list or select data by clicking the search icon.

Description Used to sort in ascending order.

View Definition Used to sort in ascending order.

12. Click the **View Definition** link. The Permission List page - General tab is displayed. For more information about Permission List, refer to the **Permission Lists** (on page 31) topic.
13. Select the **Members** tab. The Roles page - Members tab is displayed.

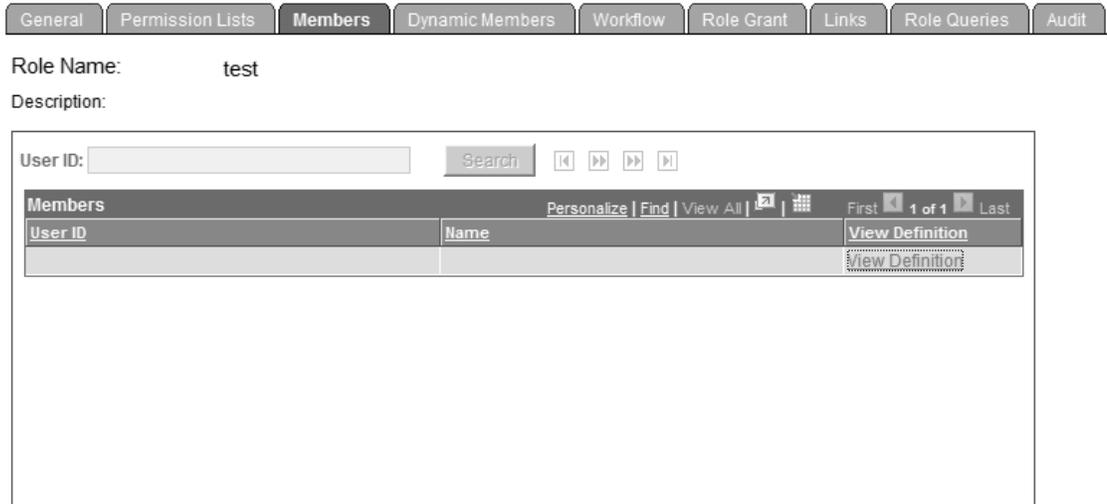
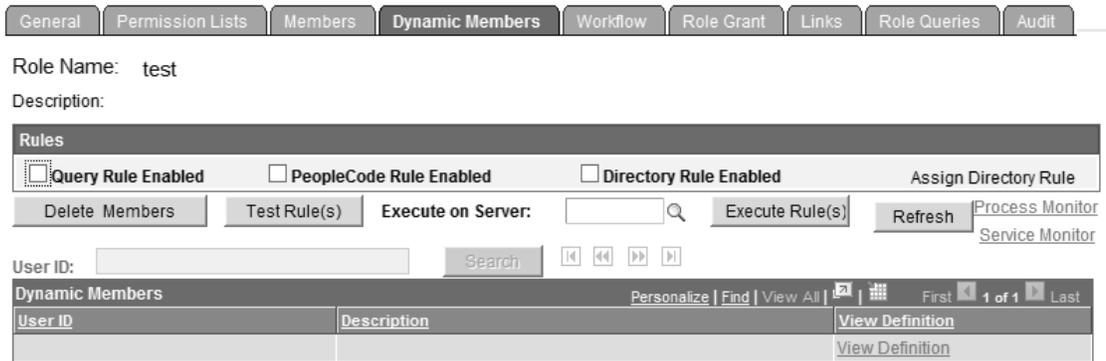


Figure 70: Roles Page - Members Tab

14. Complete the fields as follows:

Role Name	Populated with the search/add criteria entered.
Description	Populated with the description of the role name.
User ID	Non-entry field.
Members	
User ID	Populated.
Name	Populated.
View Definition	Used to sort in ascending order.

15. Select the **Dynamic Members** tab. The Roles page - Dynamic Members tab is displayed.



The screenshot shows the 'Dynamic Members' tab selected in a navigation bar. Below the navigation bar, there are fields for 'Role Name: test' and 'Description:'. A 'Rules' section contains three checkboxes: 'Query Rule Enabled', 'PeopleCode Rule Enabled', and 'Directory Rule Enabled', along with an 'Assign Directory Rule' button. Below these are buttons for 'Delete Members', 'Test Rule(s)', 'Execute on Server:' (with a search icon), 'Execute Rule(s)', 'Refresh', 'Process Monitor', and 'Service Monitor'. A 'User ID:' field with a 'Search' button and navigation icons is also present. At the bottom, a table titled 'Dynamic Members' has columns for 'User ID' and 'Description', with 'View Definition' links for each row.

Figure 71: Roles Page - Dynamic Members Tab

16. Complete the fields as follows:

Role Name	Populated based on the Role Name entered on the Roles page - General tab.
Description	Populated based on the Description entered on the Roles page - General tab.
Rules	
Query Rule Enabled	Check this box to enable the query rule.
PeopleCode Rule Enabled	Check this box to enable the people code rule.
Directory Rule Enabled	Check this box to enable the directory rule.
Execute on Server	Enter the applicable server name or select a server by clicking the search icon.
User ID	Enter the user ID.
Dynamic Members	
User ID	Populated based on the user ID entered.
Description	Populated based on the user ID entered.
View Definition	Click this link to view the definition of the dynamic members ID.

17. Click **Delete Members** to delete users.

18. Click **Test Rule(s)**. The Test Rules prompt is displayed.

19. Click **Yes** to run test rules. The Dynamic Role Test Results page is displayed.

OR

Click **No**. The Roles page - Dynamic Members tab is displayed.

Dynamic Role Test Results

Role Name: 222349 Refresh
Description: employee personal page

After executing the rules, the listed users will be assigned to the current role.

Personalize Find View All [Grid Icon] [List Icon]				
User ID	Description	Query	PCode	Dir
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 72: Dynamic Role Test Results Page

20. Click **Refresh** to refresh the page.

OR

Click **Process Monitor** to process related reports. For more information, refer to *EmpowHR*, Section 14, Report Functions.

OR

Click **Service Monitor** if applicable.

21. Select the **Workflow** tab. The Roles page - Workflow tab is displayed. User routing options are set from the Roles page - Workflow tab. This page allows users to specify routing options for a given role, thereby setting user routing rules for any user who is assigned the role.

General | Permission Lists | Members | Dynamic Members | **Workflow** | Role Grant | Links | Role Queries | Audit

Role Name: test
Description:

Workflow Routing Options

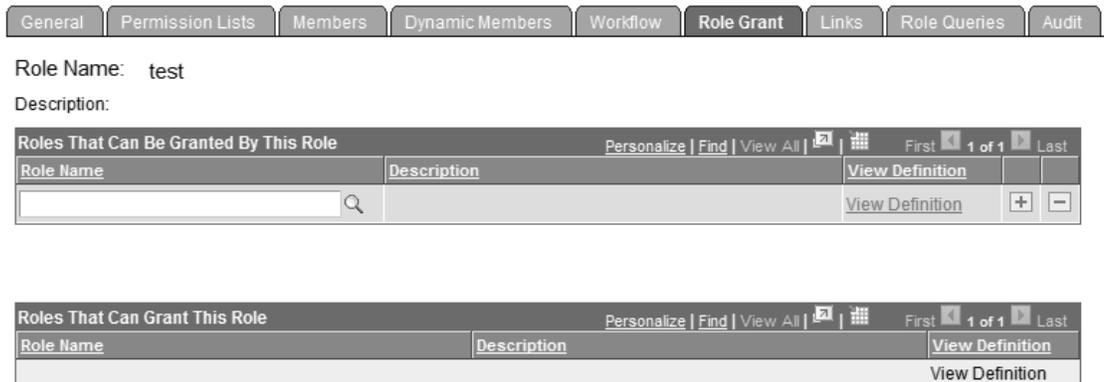
Allow notification
 Allow Recipient Lookup
 Use Query to Route Workflow

Figure 73: Roles Page - Workflow Tab

22. Complete the fields as follows:

- Role Name** Populated based on the Role Name entered on the Roles page - General tab.
- Description** Populated based on the Description entered on the Roles page - General tab.
- Workflow Routing Options**
- Allow Notification** Click this field to allow notification during the workflow process. Users can notify others of data on an *EmpowHR* page through email or work list.
- When components are designed, developers can enable the Notify toolbar on the Component Properties dialog box in *EmpowHR* Application Designer. If this option is set for a particular component, then this check box enables security administrators to enable the Notify feature per role.
- Allow Recipient Lookup** Click this field to allow recipient lookup during the workflow process. Select this field to enable role user to browse the database for the email addresses of other users in *EmpowHR*. This is available only if the Allow Notification is selected.
- Use Query to Route Workflow** Click this field to use query when routing in the workflow process. If this field is checked, the Query Name field is displayed. Select to determine workflow routing by a workflow query. This depends on the workflow scheme.

23. Select the **Role Grant** tab. The Roles page - Role Grant tab is displayed. Users other than security administrators can be given permission to assign roles.



General | Permission Lists | Members | Dynamic Members | Workflow | **Role Grant** | Links | Role Queries | Audit

Role Name: test

Description:

Roles That Can Be Granted By This Role

Role Name	Description	View Definition
		View Definition

Roles That Can Grant This Role

Role Name	Description	View Definition
		View Definition

Figure 74: Roles Page - Role Grant Tab

24. Complete the fields as follows:

- Role Name** Populated based on the Role Name entered on the Roles page - General tab.
- Description** Populated based on the Role Name entered on the Roles page - General tab.

Roles That Can Be Granted By This Role/Role Name

Enter the role name or select data by clicking the search icon. This field contains the roles that the current role is allowed to grant to other user IDs. Typically, the roles that can be granted should report to the granting role.

Roles That Can Grant This Role

Role Name

Enter the role name or select data by clicking the search icon. This group box contains the roles that can grant the current role to other user IDs.

Description

Populated based on the role name selected.

- 25. Click the **View Definition** link to view the associated definition and make sure that the appropriate definition was selected for the inclusion in the role.
- 26. Select the **Links** tab. The Roles page - Links tab is displayed.

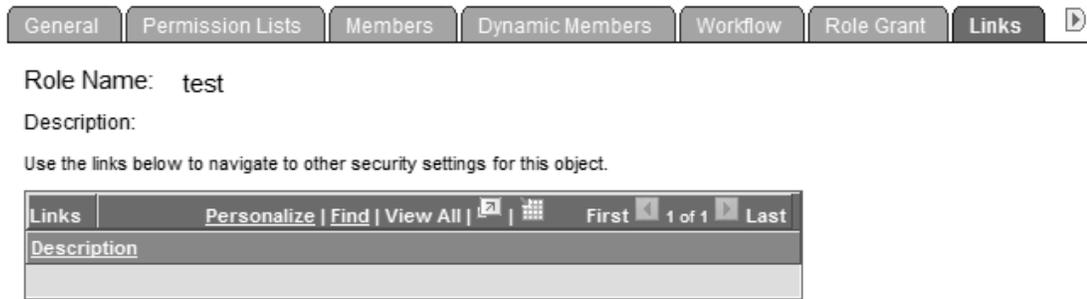


Figure 75: Roles Page - Links Tab

- 27. Complete the fields as follows:

Role Name

Populated based on the Role Name entered on the Roles page - General tab.

Description

Populated based on the Role Name entered on the Roles page - General tab.

Links

Description

Click this field to sort the list by description.

28. Click the **Role Queries** tab. The Roles page - Role Queries tab is displayed.

Members Dynamic Members Workflow Role Grant Links **Role Queries** Audit

Role Name: test

Description:

Role Specific Queries

[Role's User IDs](#)
(Which User IDs are assigned to this Role - including both static and dynamic?)

[Role's Permission Lists](#)
(To which Permission Lists does this Role belong?)

[Role's Page Access](#)
(Which pages can this Role access?)

[Role's Content Reference Access](#)
(Which access to Content References has been granted for this Role?)

[Role's Content Reference \(includes Portal\) Access](#)
(Which access to Content References (includes Portal) has been granted for this Role?)

[Role's Content Reference \(includes Menu, Component and Market\) Access](#)
(Which access to Content References (includes Menu, Component and Market) has been granted for this Role?)

[Role's Content Reference \(includes Portal, Menu, Component and Market\) Access](#)
(Which access to Content References (includes Portal, Menu, Component and Market) has been granted for this Role?)

[Role's Web Service Operation Access](#)
(Which access to Web Service Operations has been granted for this Role?)

Figure 76: Roles Page - Role Queries Tab

29. Complete the fields as follows:

Role Name	Populated based on the Role Name entered on the Roles page - General tab.
Description	Populated based on the Role Name entered on the Roles page - General tab.
Role Specific Queries	Displays a list of the following links: <ul style="list-style-type: none"> • Role's User IDs. This link displays: Which User IDs are assigned to this Role - including both static and dynamic? • Role's Permission Lists. This link displays: To which Permission Lists does this Role belong? • Role's Page Access. This link displays: Which pages can this Role access? • Role's Content Reference Access. This link displays: Which access to Content References has been granted for this Role? • Role's Content Reference (includes Portal) Access. This link displays: Which access to Content References (includes Portal) has been granted for this Role? • Role's Content Reference (includes Menu, Component and Market) Access. This link displays: Which access to Content References (includes Menu, Component and Market) has

- been granted for this Role?
- **Role's Content Reference (includes Portal, Menu, Component and Market) Access.** This link displays: Which access to Content References (includes Portal, Menu, Component and Market) has been granted for this Role?
- **Role's Web Service Operation Access.** This link displays: Which access to Web Service Operations has been granted for this Role?

Note: All available queries are documented on the Role Queries tab. Run a query by clicking the link associated with the query to be run.

Users may also choose to download the information the query returns by clicking the link corresponding to the preferred download type.

For downloading, the following options are available:

- Microsoft Excel spreadsheet - Downloads the query results as a Microsoft Excel spreadsheet (.XLS) file.
 - CSV test file - Download the query results as comma-separated values (CSV) file.
1. Select the **Audit** tab. The Roles page - Audit tab is displayed. The page is used for auditing purposes.



Figure 77: Roles Page - Audit Tab

2. Complete the fields as follows:

Role Name	Populated based on the Role Name entered on the Roles page - General tab.
Description	Populated based on the Role Name entered on the Roles page - General tab.
Audit Information	
Last Update User ID	Populated.

Last Update Date/Time Populated.

3. Click **Save** to save the information. At this point, the following options are available:

Step	Description
Click Add	Returns to the Add a New Value tab.
Click Update/Display	Returns to the Find an Existing Value tab.

Copy Roles

The **Copy Roles** component allows the user to clone an existing role.

To copy roles:

The **Copy Roles** option is used to copy a role.

1. Select the **People Tools** menu group
2. Select the **Security** menu.
3. Select the **Permission & Roles** menu item.
4. Select the **Copy Roles** component. The Role Save As page - Find an Existing Value tab is displayed.

Role Save As

Enter any information you have and click Search. Leave fields blank for a list of all values.



Find an Existing Value

▼ Search Criteria

Search by: Role Name ▼ begins with

Case Sensitive

Figure 78: Role Save As Page - Find an Existing Value Tab

5. Complete the fields as follows:

Search by Defaults to **Role Name**. To change, select data from the drop-down list.

- begins with** Enter the applicable information.
- Case Sensitive** Check this box if the criteria is case sensitive.

6. Click **Search**. A list of matches is displayed.
7. Select the applicable item on the list. The Role Save As page is displayed.

Role Save As

Save Role Name: 222349 **as:**

Figure 79: Role Save As Page

8. Complete the fields as follows:

- Save Role Name** Defaults to the item selected on the list of matches displayed after clicking **Search** on the Role Save As page - Find an Existing Value tab.
- as** Enter the new role name.

9. Click **Save** to save the copied permission list. At this point, the following options are available:

Step	Description
Click Return to Search	Returns to the Permission List Save As page - Find an Existing Value tab.
Click Refresh	Refreshes the page.

Delete Roles

The **Delete Roles** option is used to delete a role.

To delete roles:

1. Select the **People Tools** menu group.
2. Select the **Security** menu.
3. Select **Permissions & Roles**.
4. Select the **Permission Lists** menu item.

5. Select the **Delete Roles** component. The Delete Role page - Find an Existing Value tab is displayed.

Delete Role

Enter any information you have and click Search. Leave fields blank for a list of all values.

Find an Existing Value

▼ Search Criteria

Search by: Role Name begins with

Case Sensitive

Figure 80: Delete Role Page - Find an Existing Value Tab

6. Complete the fields as follows:

Search by	Defaults to Role Name . To change, select data from the drop-down list. Valid values are Description and Role Name .
begins with	Enter the applicable information.
Case Sensitive	Check this box if the criteria is case sensitive.

7. Click **Search**. A list of matches is displayed.
8. Select the applicable item on the list. The Delete Role page is displayed.

Delete Role

Role Name: 222349

Delete Role

Figure 81: Delete Role Page

9. Complete the Role Name field as follows:

Role Name	Populated based on the item selected on the Role Save As page - Find an Existing Value tab.
------------------	---

10. Click **Delete Role**. A Delete Role Confirmation popup appears.
11. Click **OK** to delete the permission list and return to the Delete Role page - Find an Existing Value tab.

OR

Click **Cancel** to cancel the deletion and return to the Delete Role page - Find an Existing Value tab.

Execute Role Rules

The **Execute Role Rules** option is used to execute role rules. The Process Monitor and Message Monitor are both available with this option.

To execute role rules:

1. Select the **People Tools** menu group.
2. Select the **Security** menu.
3. Select the **Permissions & Roles** menu item.
4. Select the **Execute Role Rules** component. Dynamic Role Rules page is displayed.

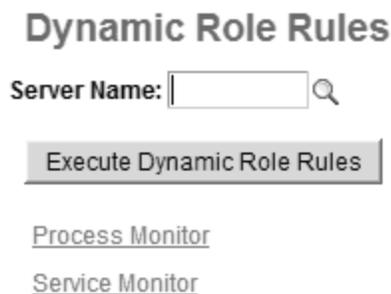


Figure 82: Dynamic Role Rules Page

5. Complete the Server Name field as follows:

Server Name	Enter the applicable information or search data by clicking the search icon.
--------------------	--

6. Click **Execute Dynamic Role Rules**. The information is saved.

Password Configuration

This section provides information and procedures necessary for defining and configuring password control.

Password controls help ensure access to *EmpowHR*.

For more information see:

Password Controls	74
Forgotten Password Email Text	77
Forgotten Password Hint	79
Delete Forgotten Password Hint	80

Password Controls

The Password Controls page allows administrators to set any password restrictions such as duration or minimum length of a password for end users. The following table provides a list of available password control options and a description of each.

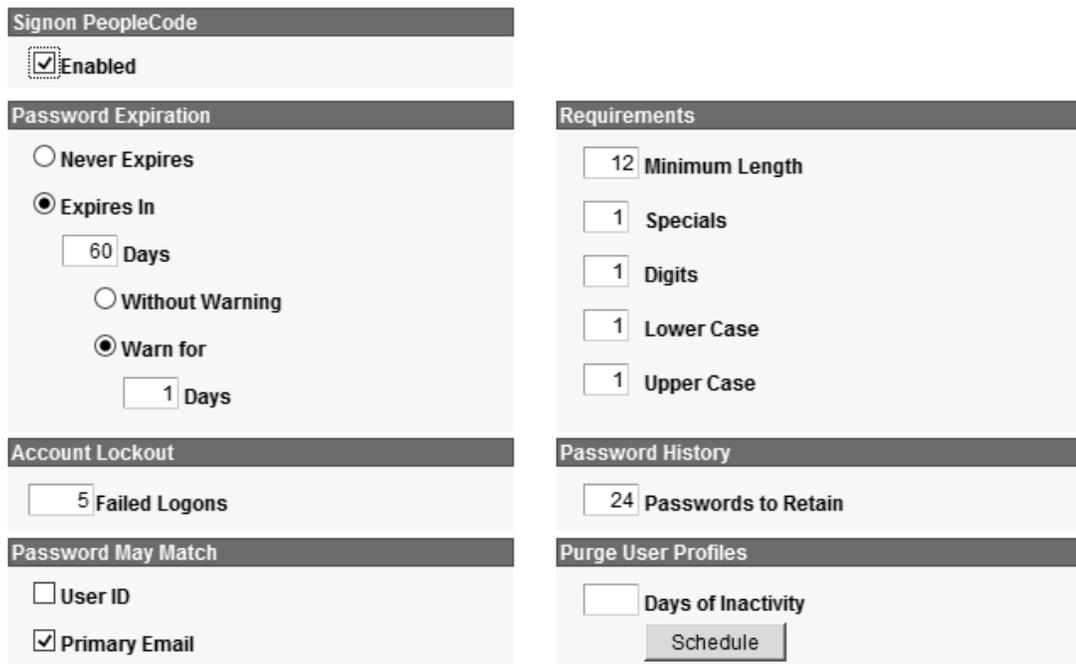
Password Control Option	Description
Enable Signon PeopleCode	<p>Select this checkbox to enable the following <i>EmpowHR</i> password controls: Password Expiration and Account Lockout. The other password controls are not enabled by this box.</p> <p>Leave the checkbox clear if no password controls should be in place (unless another third party utility that performs equivalent features is in place).</p>
Password Expiration	<p>Use this option to specify the age allowed for passwords.</p> <ul style="list-style-type: none"> • Select the Password Never Expires checkbox if you do not want the password to expire. • Define a number of days (between 1 and 365) that a password is valid by, selecting the Password Expires in ___ Days option. Users logging on after a password expires must change their password to log on to <i>EmpowHR</i>. <p>This option also allows for the specification of the duration that <i>EmpowHR</i> wants to notify the user when the password is about to expire.</p>
Account Lockout	<p>Use this option to enable locking an account after a number of failed logon attempts. (For example, if the set Maximum Logon Attempts value is 3 and the user fails three logons, the user is automatically locked out of <i>EmpowHR</i>.)</p> <p>If a 0 (zero) is entered, the account will not be locked out due to erroneous attempts.</p> <p>After the account is locked out, a system security administrator must open the user profile and clear the Account Lockout checkbox manually.</p>
Miscellaneous	<p>Use this option to check the Allow password to match User ID checkbox to enable administrators to make sure users do not use their own user ID as a password. This helps prevent hackers from guessing passwords based on a list of employee names.</p> <p>In general, this checkbox should not be selected as it is very risky to allow</p>

	passwords and user IDs to match.
Minimum Length	Use this control to specify the minimum allowed length for passwords in the application. The value of 0 (zero) indicates there is no minimum length required; however, <i>EmpowHR</i> will still require the Password field not to be blank.
Character Requirements	Use this section to specify the character requirements for your passwords. Administrators can require a set number of digits or special characters within a password. Special characters, or "specials", refer to symbols such as # and @, and digits refer to number (integers), such as 1 or 2.
Purge Inactive User Profiles	Use this option to enable the purging of user profiles that have not been used in a specified amount of time. This aids in general housekeeping.

To access the Password Controls page:

1. Select the **People Tools** menu group.
2. Select the **Security** menu.
3. Select the **Password Configuration** menu item.
4. Select the **Password Controls** component. The Password Controls page is displayed.

Password Controls



Signon PeopleCode
 Enabled

Password Expiration
 Never Expires
 Expires In
 60 Days
 Without Warning
 Warn for
 1 Days

Account Lockout
 5 Failed Logons

Password May Match
 User ID
 Primary Email

Requirements
 12 Minimum Length
 1 Specials
 1 Digits
 1 Lower Case
 1 Upper Case

Password History
 24 Passwords to Retain

Purge User Profiles
 Days of Inactivity
 Schedule

Figure 83: Password Controls Page

5. Complete the fields as follows:

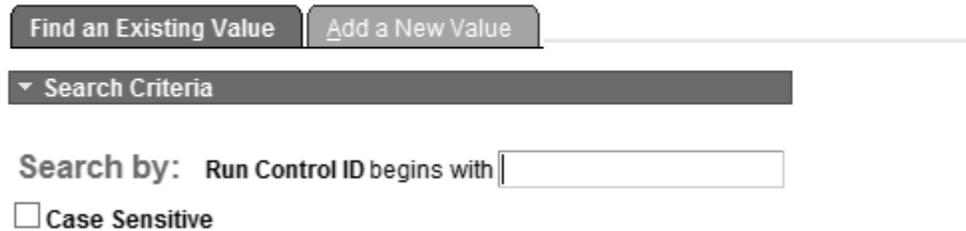
Enable Signon PeopleCode	Check this box to enable the Password Expiration and Account Lockout password controls. The Password Expiration and Account Lockout options are not editable.
Password Expiration	
Password Never Expires	Select if the password should never expire.
Password Expires in Days	Select if the password will expire and enter the number of days the password will be valid. When this option is selected, the days field is activated.
<hr/> Note: Passwords should expire after 90 days. <hr/>	
Do not warn of expiration	Select if there should be no warning of the expiration of the password.
Warn for Days	Select and specify the length of the warning period. When this option is selected, the days field is activated. Enter the number of days when the warning for the password expiration should display.
Account Lockout	
Maximum Logon Attempts	Enter the number of logon attempts before the user is locked out.
Miscellaneous	
Allow password to match UserID	Check this box if the user is allowed to match the user ID to the password.
Minimum Length	
Minimum Password Length	Enter the minimum number of characters designated for the password length.
Character Requirements	
Required Number of Specials	Enter the number of special characters designated for the password.
Required Number of Digits	Enter the required number of digits designated for the password.
Purge Inactive User Profiles	
After: Days	Enter the number of days a password can remain inactive before it is purged for the system.
Password History	
Number of Passwords to Retain	Enter the number of passwords to be retained in history.

- Click **Save**. This function must be performed prior to selecting **Schedule**.

7. Click **Schedule**. The Purge Inactive User Profiles page - Find an Existing Value tab is displayed.

Purge Inactive User Profiles

Enter any information you have and click Search. Leave fields blank for a list of all values.



The screenshot shows the 'Purge Inactive User Profiles' page with the 'Find an Existing Value' tab selected. Below the tabs is a 'Search Criteria' dropdown menu. The 'Search by:' field is set to 'Run Control ID begins with' with an empty text input field. The 'Case Sensitive' checkbox is unchecked.

Figure 84: Purge Inactive User Profiles Page - Find an Existing Value Tab

8. Complete the field as follows:

Search by: Run Control ID begins with Enter the run control ID.

9. Click **Search**. The Purge Inactive User Profiles page is displayed.

Purge Inactive User Profiles

Purge the system of user profiles that have not been used in a specified amount of time. This aids in general housekeeping.

Go to: [Setup Purge Frequency for Inactive User Profiles](#)



The screenshot shows the 'Purge Inactive User Profiles' page with the 'Run Control ID:' field containing 'test'. Below the field are two links: 'Report Manager' and 'Process Monitor'. A 'Run' button is visible on the right side of the page.

Figure 85: Purge Inactive User Profiles Page

Forgotten Password Email Text

Before the application emails a new randomly generated password, verify the user's identify. The Forgotten Password feature enables the posting of a standard question to users requesting a new password to verify the user's authenticity. If the user enters the appropriate response, the application will automatically email a new password.

When a user has forgotten a password, the application sends the user a new password via email. There may be numerous password strings, but typically, all new passwords are sent using the same email message template. Because of this, *EmpowHR* provides a separate page for composing the standard email text that is used for the template.

To access the Forgot My Password Email page:

1. Select the **People Tools** menu group.
2. Select the **Security** menu.
3. Select the **Password Configuration** menu item.
4. Select the **Forgotten Password Email Text** component. The Forgot My Password Email Text page is displayed.

Forgot My Password Email Text

Enter the text of the email to be sent with the user's new password.
Please include the exact string <<%PASSWORD>> in the email text.
This will be replaced with the new randomly generated password.

Email Text:

The screenshot shows a rich text editor interface. The toolbar includes icons for undo, redo, bold, italic, underline, font color, background color, bulleted list, numbered list, indent, and outdent. The text area contains the text: "New Password Generated from EMPOWHR is: <".

Figure 86: Forgot My Password Email Text Page

5. Complete the field as follows:

Email Text

Compose the standard text to be sent to the users who have forgotten their passwords and have requested a new one.

Add the following text string in the Email Text edit box:

<<%PASSWORD>>

This is where the system inserts the new password. The %PASSWORD variable resolves to the generated value.

6. Click **Save**.

OR

Click **Refresh** to clear the window.

Forgotten Password Hint

Password hints are set up for users who have forgotten their password. By using these hints correctly, users access the Forgot My Password page. The user answers the question (Challenge Questions) correctly and gets a new password sent via email.

To access the Forgot My Password Hint page:

1. Select the **People Tools** menu group.
2. Select the **Security** menu.
3. Select the **Password Configuration** menu item.
4. Select the **Forgotten Password Hint** component. The Forgot My Password Hint page - Find an Existing Value tab is displayed.

Forgot My Password Hint

Enter any information you have and click Search. Leave fields blank for a list of all values.



Figure 87: Forgot My Password Hint Page - Find an Existing Value Tab

5. Complete the field as follows:

Search by: Password Hint ID begins with Enter the search criteria to find an existing password hint.

6. Click **Search**. The Forgot My Password Hint page is displayed

OR

Select the **Add a New Value** tab to add a new Password Hint. The Forgot My Password Hint page - Add a New Value tab is displayed.

Forgot My Password Hint

Password Hint ID:

Figure 88: Forgot My Password Hint Page - Add a New Value Tab

- Complete the field as follows:

Password Hint ID Enter the three-position password hint ID.

- Click **Add**. The Forgot My Password Hint page is displayed.

Forgot My Password Hint

Password Question ID: TST

Active:

*Question:

Figure 89: Forgot My Password Hint Page

- Complete the field as follows:

Password Question ID Populated based upon the search criteria entered.

Active Verify the Active checkbox is selected.

***Question** Enter the verification question.

- Click **Save** to save the question.

Delete Forgotten Password Hint

This section explains how to delete a forgotten password hint.

To access the Delete Forgot My Password Hint page:

1. Select the **People Tools** menu group.
2. Select the **Security** menu.
3. Select the **Password Configuration** menu item.
4. Select the **Delete Forgotten Password Hint** component. The Delete Forgot My Password Hint page - Find an Existing Value tab is displayed.

Delete Forgot My Password Hint

Enter any information you have and click Search. Leave fields blank for a list of all values.



Figure 90: Delete Forgot My Password Hint Page - Find an Existing Value Tab

5. Complete the field as follows:

Search by: Password Hint ID begins with Enter the applicable information.

6. Click **Search**. The Delete Forgot My Password Hint page is displayed with applicable Password Hint ID based upon the search criteria entered. This is a read-only page.

Delete Forgot My Password Hint

Password Hint ID: 001
Question: What is your pet's name?
Last Update Date/Time: 10/30/01 9:46:31AM
Last Update User ID: XXXXXX

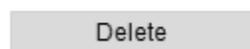


Figure 91: Delete Forgot My Password Hint Page

7. Click **Delete** to delete the password hint. You are returned to the Delete Forgot My Password Hint page - Find a Existing Value tab is displayed.
8. Click **Save** to save the information.

Security Objects

This section allows the user to maintain objects such as single signon and digital certificates.

For more information see:

User Profile Types	82
Tables to Skip	84
Security Links	85
Digital Signature	87
Single Signon.....	90
Signon PeopleCode	91

User Profile Types

To update/add a user profile type:

1. Select the **People Tools** menu group.
2. Select **Security**.
3. Select the **Security Objects** menu.
4. Select the **User Profile Types** component. The User Profile Types page - Find an Existing Value tab is displayed.

The screenshot shows the 'User Profile Types' page interface. At the top, it says 'User Profile Types' and 'Enter any information you have and click Search. Leave fields blank for a list of all values.' Below this are two buttons: 'Find an Existing Value' and 'Add a New Value'. Underneath the buttons is a dropdown menu labeled 'Search Criteria'. At the bottom, there is a 'Search by:' label followed by the text 'ID Type begins with' and an empty text input field.

Figure 92: User Profile Types Page - Find an Existing Value Tab

5. Complete the field as follows:

Search by: ID Type begins with Enter the ID Type.

- Click **Search** The User Profile Types page is displayed.

OR

Select the **Add a New Value** tab. The User Profile Types page - Add a New Value tab is displayed.

User Profile Types

ID Type:

Figure 93: User Profile Types Page - Add a New Value Tab

- Complete the field as follows:

ID Type Enter the ID Type to be added.

- Click **Add**. The User Profile Types page is displayed.

User Profile Types

ID Type: Enabled?

*Description: *Sequence number:

Long Description:

Field Information				Personalize Find View All [?] [grid]		First	1-2 of 2	Last
*Field Name		*Record (Table) Name		Description	Fieldname			
1	SETID	SETID_TBL	DESCR					
2	BIDDER_ID	AUC_BID_CONTACT	NAME1					

Figure 94: User Profile Types Page

- Complete the fields as follows:

ID Type Populated from the search/add criteria entered.

Enabled?	Check this box to enable the user profile.
*Description	Enter the description of the user profile type.
*Sequence number	Enter the sequence number.
Long Description	Enter the narrative long description for the user profile type.
Field Information	
*Field Name	Enter the name of the user profile or select data by clicking the search icon.
*Record (Table) Name	Enter the table name or select data by clicking the search icon.
Description Fieldname	Enter the description of the field name or select data by clicking the search icon.

10. Click **Save** to save the information.

Tables to Skip

The Bypass Tables page lists the tables to be bypassed during a user profile deletion.

To bypass a table:

1. Select the **People Tools** menu group.
2. Select the **Security Objects** menu.
3. Select the **Tables to Skip** component. The Bypass Tables page. The table(s) listed will be bypassed.

Bypass Tables



Bypass these tables during User Profile Deletion		Personalize	Find	1 of 1	First	Last
Record (Table) Name	Record Description					
1 PRG_USR_PROFILE	User Profile Purge History				+	-

Figure 95: Bypass Tables Page

4. Click **Save** to save the information.

Security Links

To enter a security link:

1. Select the **People Tools** menu group.
2. Select the **Security** menu.
3. Select the **Security Objects** menu item.
4. Select the **Security Links** component. The Security Links page - User tab is displayed.

Active Flag	Description	*Menu Name	*Menu Bar Name	Bar Item Name	Item Name	Test
<input type="checkbox"/>						Test

Figure 96: Security Links Page - User Tab

5. Complete the fields as follows:

User Security Links

- Active Flag** Check this box if applicable.
- Description** Enter the applicable description.
- *Menu Name** Enter the menu name or select data by clicking the search icon.
- *Menu Bar Name** Enter the menu bar name or select data by clicking the search icon.
- Bar Item Name** Enter the bar item name or select data by clicking the search icon.
- Item Name** Enter the item name or select data by clicking the search icon.

Note: You can click the **Test** link from any tab to display the Review AP Extract-Headers page - Find an Existing Value tab. This page allows you to search by SetID, Vendor ID, and Invoice Number.

6. Select the **My Profile** tab. The Security Links page - My Profile tab is displayed.

Active Flag	Description	*Menu Name	*Menu Bar Name	Bar Item Name	Item Name	Test
<input type="checkbox"/>						Test

Figure 97: Security Links Page - My Profile Tab

7. Complete the fields as follows:

My Profile User Security Links

- Active Flag** Check this box if applicable.
- Description** Enter the applicable description.
- *Menu Name** Enter the menu name or select data by clicking the search icon.
- *Menu Bar Name** Enter the menu bar name or select data by clicking the search icon.
- Bar Item Name** Enter the bar item name or select data by clicking the search icon.
- Item Name** Enter the item name or select data by clicking the search icon.

8. Select the **Role** tab. The Security Links page - Role tab is displayed.



Figure 98: Security Links Page - Role Tab

9. Complete the fields as follows:

Role Security Links

- Active Flag** Check this box if applicable.
- Description** Enter the applicable description.
- *Menu Name** Enter the menu name or select data by clicking the search icon
- *Menu Bar Name** Enter the menu bar name or select data by clicking the search icon.
- Bar Item Name** Enter the bar item name or select data by clicking the search icon.
- Item Name** Enter the item name or select data by clicking the search icon.

10. Select the **Permission List** tab. The Security Links page - Permission List tab is displayed.



Figure 99: Security Links Page - Permission List Tab

11. Complete the fields as follows:

Permission List Security Links

Active Flag	Check this box if applicable.
Description	Enter the applicable description.
*Menu Name	Enter the menu name or select data by clicking the search icon.
*Menu Bar Name	Enter the menu bar name or select data by clicking the search icon.
Bar Item Name	Enter the bar item name or select data by clicking the search icon.
Item Name	Enter the item name or select data by clicking the search icon.

12. Click **Save**.

Digital Signature

To view digital signatures:

1. Select the ***People Tools*** menu group.
2. Select the ***Security*** menu.
3. Select the ***Security Objects*** menu item.

- Select the **Digital Signature** component. The Digital Certificates page is displayed. This page displays the type of certificate, *alias and *issuer alias, and valid to (date and time).

Digital Certificates

Digital Certificates				Personalize	Find	First	1-19 of 19	Last
Type	*Alias	*Issuer Alias	Valid to	Links				
Root CA	GTE CyberTrust Global Root	GTE CyberTrust Global Root		Detail	+	-		
Root CA	GTE CyberTrust Root	GTE CyberTrust Root		Detail	+	-		
Root CA	KeyWitness Root	KeyWitness Root		Detail	+	-		
Root CA	PeopleTools TEST root CA	PeopleTools TEST root CA	11/20/23 9:36:28AM	Detail	+	-		
Root CA	Root SGC Authority	Root SGC Authority	12/31/09 11:00:00PM	Detail	+	-		
Root CA	Thawte Personal Basic	Thawte Personal Basic	12/31/20 3:59:59PM	Detail	+	-		
Root CA	Thawte Personal Premium	Thawte Personal Premium	12/31/20 3:59:59PM	Detail	+	-		
Root CA	Thawte Premium Server	Thawte Premium Server	12/31/20 3:59:59PM	Detail	+	-		
Root CA	Thawte Server	Thawte Server	12/31/20 3:59:59PM	Detail	+	-		
Root CA	Verisign Class 1	Verisign Class 1	01/07/20 3:59:59PM	Detail	+	-		
Root CA	Verisign Class 1 - G2	Verisign Class 1 - G2	05/18/20 4:59:59PM	Detail	+	-		
Root CA	Verisign Class 2	Verisign Class 2	08/01/28 4:59:59PM	Detail	+	-		
Root CA	Verisign Class 2 - G2	Verisign Class 2 - G2	05/18/18 4:59:59PM	Detail	+	-		
Root CA	Verisign Class 3	Verisign Class 3	08/01/28 4:59:59PM	Detail	+	-		
Root CA	Verisign Class 3 - G3	Verisign Class 3 - G3	05/18/18 4:59:59PM	Detail	+	-		
Root CA	Verisign Class 3 Public Primary CA	Verisign Class 3 Public Primary CA	08/01/28 4:59:59PM	Detail	+	-		
Root CA	Verisign Class 4	Verisign Class 4	05/18/18 4:59:59PM	Detail	+	-		

Figure 100: Digital Certificates Page

5. Click the **Detail** link. The Certificate Detail page is displayed.



The screenshot shows a web interface titled "Certificate Detail". It is divided into two main sections: "Subject Information" and "Certificate Information".

Subject Information

- Common Name:
- Org Unit:
- Organization:
- Locality:
- State/Province: Country: US

Certificate Information

- Serial Number:
- Fingerprint:
- Valid from 08/12/1998 18:29:00 to 08/13/2018 17:59:00
- Algorithm:
- Description: (This field is empty and has a scroll bar on the right side.)

Figure 101: Certificate Detail Page

6. Complete the fields as follows:

Subject Information

- | | |
|-----------------------|--|
| Common Name | Populated with the common name for the certificate root. |
| Org Unit | Populated with the organization unit name. |
| Organization | Populated with the organization name. |
| Locality | Populated with the locality, if applicable. |
| State/Province | Populated with the State providence, if applicable. |
| Country | Populated with the country. |

Certificate Information

- | | |
|----------------------|--|
| Serial Number | Type the serial number of the certificate. |
|----------------------|--|

Fingerprint	Populated with the fingerprint of the person that the certificate relates to.
Valid from	Valid dates and the time the certificate was issued.
Algorithm	Methods used to issue the certificate.
Description	Type the description of the algorithm.

- Click **Review** to review the certificate.
- Click **Export**. The Export Certificate page is displayed.
- Click **OK**. At this point, the following options are available:

Step	Description
Click Cancel	Returns to the Certificate Detail - GTE CyberTrust Global Root page.
Click Refresh	Refreshes the page.

Single Signon

This option allows the security officer to add functionality to a profile to accomplish a single signon.

To create a Single Signon:

- Select the **People Tools** menu group.
- Select the **Security** menu.
- Select the **Security Objects** menu item.
- Select the **Single Signon** component. The Single Signon page is displayed.

Single Signon

Authentication Token expiration time

Expiration Time in minutes: Valid values are 1 - 10,000

Trust Authentication Tokens issued by these Nodes			
Message Node Name	Description	Local Node	
PSFT_CR	PS CRM - Local Node		+ -
PSFT_HR	PS HRMS - Local Node	1	+ -

Figure 102: Single Signon Page

- Complete the fields as follows:

Authentication Token expiration time

Expiration Time in minutes Number of minutes from **1** to **10 , 000**.

Trust Authentication Tokens issued by these Nodes

Message Node Name Enter the message node name or select data by clicking the search icon.

Description Populated with the description corresponding to the Message Node Name.

Local Node Populated with the local node.

6. Click **Save**.

OR

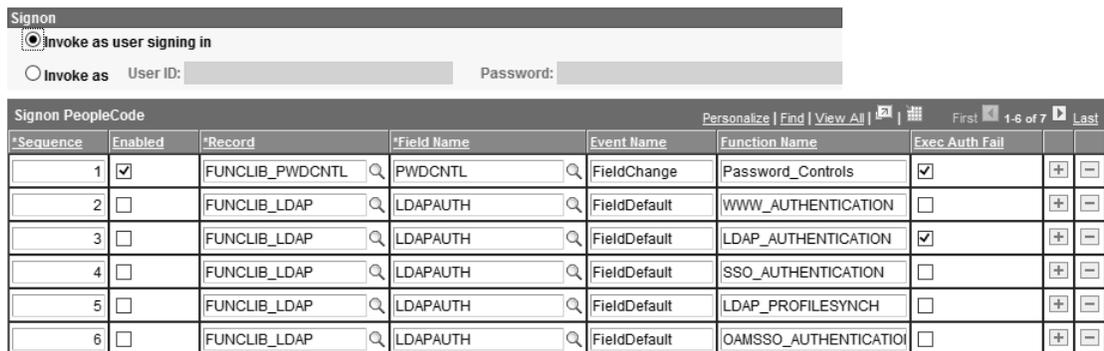
Click **Refresh** to refresh the page.

Signon PeopleCode

To create a Signon PeopleCode:

1. Select the **People Tools** menu group.
2. Select the **Security** menu.
3. Select the **Security Objects** menu item.
4. Select the **Signon PeopleCode** component. The Signon PeopleCode page is displayed.

Signon PeopleCode



*Sequence	Enabled	*Record	*Field Name	Event Name	Function Name	Exec Auth Fail
1	<input checked="" type="checkbox"/>	FUNCLIB_PWDCNTL	PWDCNTL	FieldChange	Password_Controls	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	WWW_AUTHENTICATION	<input type="checkbox"/>
3	<input type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	LDAP_AUTHENTICATION	<input checked="" type="checkbox"/>
4	<input type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	SSO_AUTHENTICATION	<input type="checkbox"/>
5	<input type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	LDAP_PROFILESYNCH	<input type="checkbox"/>
6	<input type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	OAMSSO_AUTHENTICATIOI	<input type="checkbox"/>

Figure 103: Signon PeopleCode Page

5. Complete the fields as follows:

Signon

Invoke as user signing in Select if applicable.

Invoke as Select if applicable. If you select this option, the User ID and Password fields must be completed.

User ID Enter the user ID if the Invoke as radio button is selected.

Password Enter the password if the Invoke as radio button is selected.

Signon PeopleCode

***Sequence** Populated with the sequence number.

Enabled Check this box if the signon is enabled.

***Record** Enter the applicable record description or change by clicking the search icon.

***Field Name** Enter the field name or change by clicking the search icon.

Event Name Defaults to the event.

Function Name Populated with the function name.

Exec Auth Fail Check this box if applicable.

6. Click **Save**.

OR

Click **Refresh** to refresh the page.

Query Security

In query trees, include all record components that users should be able to query. Not all record components must be included in the same query tree. Use the **Query Access Manager** option to create query trees to search for existing query trees. How the contents of the query trees are organized depends upon the needs of the Agency and users.

This section allows the user to define query security.

For more information see:

Query Access Manager	93
Query Access List Cache	95

Query Access Manager

To use Query Access Manager:

1. Select the **People Tools** menu group.
2. Select the **Query Security** menu.
3. Select the **Query Access Manager** component. The Query Access Manager page - Basic Search is displayed.



Figure 104: Query Access Manager Page - Basic Search

4. Complete the fields as follows:

***Search By** Defaults to **Tree Name**. To change, select data from the drop-down list.

Tree Name Enter the tree name.

5. Click **Search**.

OR

Select **Create a New Tree**. The Tree Definition and Properties page is displayed.

Tree Definition and Properties

*Tree Name:

*Structure ID:

*Effective Date: *Status:

*Description:

*Category:

*Use of Levels: [Performance Options](#)

*SetID:

Audits	Item Counts
<input type="checkbox"/> All Detail Values in this Tree <input type="checkbox"/> Allow Duplicate Detail Values <input type="button" value="Perform Audits"/>	Node Count: 1 Leaf Count: 1 Level Count: 2 Branch Count: 0

Figure 105: Tree Definition and Properties Page

6. Complete the fields as follows:

- *Tree Name Enter the tree name.
- *Structure ID Defaults to **Access-Group** and cannot be changed.
- *Effective Date Populated with the current date. To change, select a date from the calendar icon.
- *Status Defaults to **Active**. To change, select data from the drop-down list. Valid values are **Active** and **Inactive**.
- *Description Enter the applicable description of the tree name.
- *Category Defaults to **Default** or change by clicking the search icon.
- *Use of Levels Defaults to **Strictly Enforced**. Change by clicking the down arrow.

Audits

All Detail Values in this Tree Check this box if applicable.

Allow Duplicate Detail Values Check this box if applicable.

Item Counts

Node Count Populated.

Leaf Count Populated.

Level Count Populated.

Branch Count Populated.

7. Click **OK**.

OR

Click **Refresh** to refresh the page.

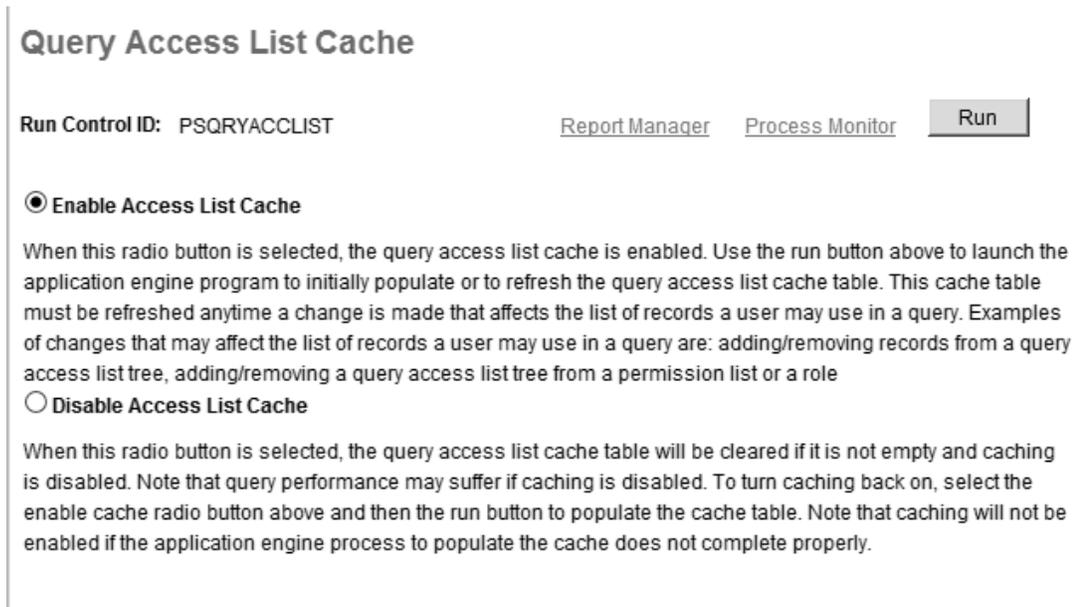
Query Access List Cache

An additional batch process is available for users who work with Query manager, Crystal Reports, and PS/Vision. *EmpowHR* moves quickly to retrieve the queries that match the designated search criteria if the query access list cache is enabled.

To use Query Access Manager:

1. Select the **People Tools** menu group.
2. Select **Security**.
3. Select the **Query Security** menu.

- Select the **Query Access List Cache** component. The Query Access List Cache page is displayed.



Query Access List Cache

Run Control ID: PSQRYACCLIST [Report Manager](#) [Process Monitor](#)

Enable Access List Cache

When this radio button is selected, the query access list cache is enabled. Use the run button above to launch the application engine program to initially populate or to refresh the query access list cache table. This cache table must be refreshed anytime a change is made that affects the list of records a user may use in a query. Examples of changes that may affect the list of records a user may use in a query are: adding/removing records from a query access list tree, adding/removing a query access list tree from a permission list or a role

Disable Access List Cache

When this radio button is selected, the query access list cache table will be cleared if it is not empty and caching is disabled. Note that query performance may suffer if caching is disabled. To turn caching back on, select the enable cache radio button above and then the run button to populate the cache table. Note that caching will not be enabled if the application engine process to populate the cache does not complete properly.

Figure 106: Query Access List Cache Page

- Complete the fields as follows:

Run Control ID	Populated based upon the user's log on information.
Enable Access List Cache	Select this field if the access should be enabled.
Disable Access List Cache	Select this field if the access should be disabled.

- Click **Report Manager**. For more information on Report Manager, refer to *EmpowHR*, Section 14, Report Functions.
- Click **Process Monitor**. For more information on Process Monitor, refer to *EmpowHR*, Section 14, Report Functions.
- Click **Run**. For more information on Run, refer to *EmpowHR*, Section 14, Report Functions.

Common Queries

This section allows the user to maintain (via links) user IDs, roles, permission lists, and People Tools object security queries.

To use Common Queries:

1. Select the **People Tools** menu group.
2. Select the **Security** menu.
3. Select the **Common Queries** component. The Review Security Information page is displayed.

Review Security Information

User ID Queries

Queries specific to a User ID.

Role Queries

Queries specific to a Role.

Permission List Queries

Queries specific to a Permission List.

PeopleTools Objects Queries

Queries specific to a PeopleTools object.

Definition Security Queries

Queries specific to Definition Security.

Access Log Queries

Queries specific to log-in/log-out activity

Figure 107: Review Security Information Page

Below is a list of links:

- **User ID Queries** includes queries specific to a user ID.
- **Role Queries** includes queries specific to a role.
- **Permission List Queries** includes queries specific to a permission list.
- **PeopleTools Objects Queries** includes queries specific to a PeopleTools object.
- **Definition Security Queries** includes queries specific to definition security.
- **Access Log Queries** includes queries specific to login/logout activity.

Mass Change Operator Security

This section allows the user to set mass change operator security.

To set mass change operator security:

1. Select the **People Tools** menu group.
2. Select the **Security** menu.
3. Select the **Mass Change Operator Security** component. The Mass Change Operator Security page - Find an Existing Value tab is displayed.

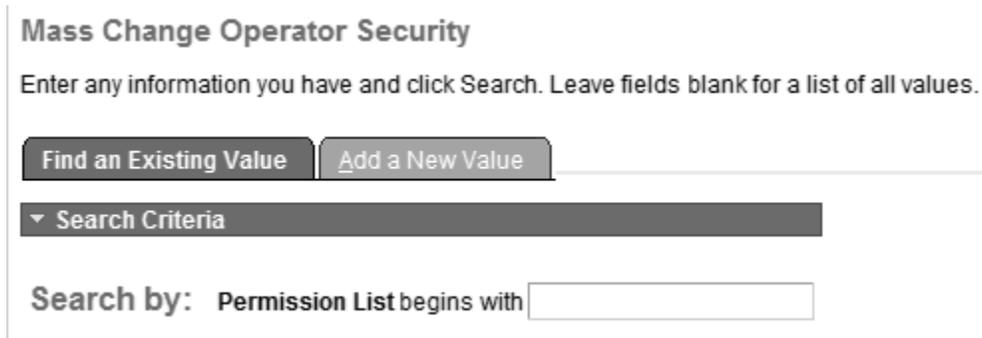


Figure 108: Mass Change Operator Security Page - Find an Existing Value Tab

4. Complete the field as follows:

Search by: Permission List begins with Enter the permission list.

5. Click **Search**. The Security tab page is displayed.

OR

Select the **Add a New Value** tab. The Mass Change Operator Security page - Add a New Value tab is displayed.

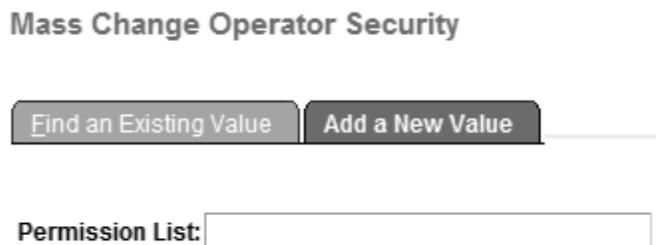


Figure 109: Mass Change Operator Security Page - Add a New Value Tab

6. Complete the field as follows:

Permission List Enter the permission list.

- Click **Add**. The Security tab page is displayed.

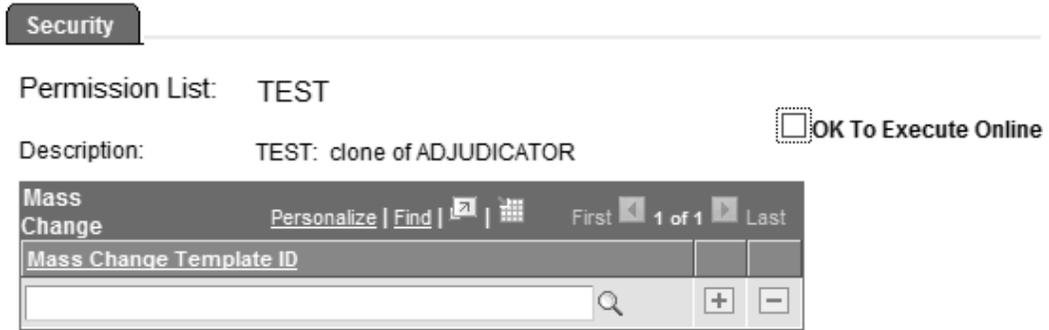


Figure 110: Security Tab Page

- Complete the fields as follows:

Permission List Populated based on the search/add criteria entered.

Description Populated based on the search/add criteria entered.

OK to Execute Online Check this box if applicable.

Mass Change

Mass Change Template ID Enter the mass change template ID or select data by clicking the search icon.

- Click **Save**. At this point, the following options are available:

Step	Description
Click Notify	Notifies the next individual in the workflow.
Click Add	Adds an additional mass change operator security.
Click Update Display	Updates the page.

Tree Manager

Trees provide an easy way to create, maintain, and visualize the roll-up relationships of data throughout *EmpowHR*. They logically organize and provide a visual summary of detailed data while allowing updates to apply changes that reflect the user’s data organization.

Trees are effective dated, so that they can be used with past, present, or future dates when reporting on current or historical data. Trees can also be used to test different scenarios and strategies. They will not pick up data with an effective date after the tree’s effective date.

Trees are comprised of Nodes, which are grouped fields, values, or other nodes that logically belong together for reporting purposes.

Term	Definition
Root Node	Parent folder or the highest level of a hierarchy.
Parent Node	Node that has other nodes reporting to it.
Child Node	Node that reports to a parent mode.
Sibling Node	Nodes at the same level that represents children reporting to the same parent node.

The following actions can be performed on the **Tree Manager** component on the tree that is selected by using links and images on the navigation bar (the horizontal blue bar at the top of the tree).

Action	Description
Collapse	Closes all of the visible nodes except for the root node. The root node is always expanded.
Expand All	Expands all of the nodes on the tree, so that the entire tree or branch hierarchy is visible. Expands all parent/child relationships, but the tree hierarchy is still presented one page at a time.
Find	Accesses the Find an Existing Value tab and search for nodes and detail values.

The **Tree Manager** option is displayed when you select **Tree Manager** from the main menu.

This section includes the following topics:

Introduction to Tree Manager	102
Tree Viewer.....	106
Tree Auditor	108

Tree Structure110
Tree Utilities112

Introduction to Tree Manager

To find an existing tree on the Tree Manager page:

1. Select the **Tree Manager** menu group.
2. Select the **Tree Manager** component. The Tree Manager page - Find an Existing Tree tab is displayed.

Tree Manager
Enter any information you have and click Search. Leave fields blank for a list of all values.

Find an Existing Tree Create New Tree

▼ Search Criteria

Search by: begins with

Figure 111: Tree Manager Page - Find an Existing Tree Tab

3. Complete the fields as follows:

Search by Defaults to **Tree Name**. To change, select data from the drop-down list.

begins with Enter the information that corresponds to the Search by valid values.

4. Click **Search**. The Tree Manager page is displayed.

OR

5. Select the **Create New Tree** tab. The Tree Manager page - Create New Tree tab is displayed.



Tree Manager

Find an Existing Tree Create New Tree

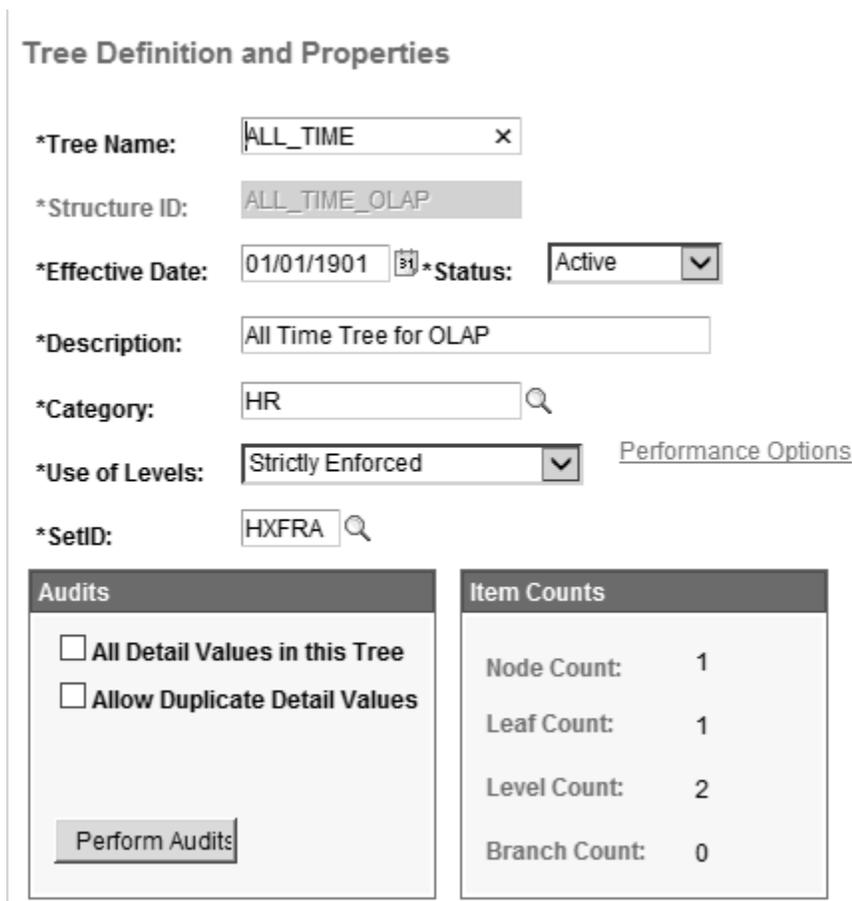
Tree Name:

Figure 112: Tree Manager Page - Create New Tree Tab

6. Complete the field as follows:

Tree Name Enter the name of the tree to be added.

7. Click **Add**. The Tree Definition and Properties page is displayed.



Tree Definition and Properties

*Tree Name: x

*Structure ID:

*Effective Date: *Status:

*Description:

*Category: 🔍

*Use of Levels: [Performance Options](#)

*SetID: 🔍

Audits	
<input type="checkbox"/>	All Detail Values in this Tree
<input type="checkbox"/>	Allow Duplicate Detail Values
<input type="button" value="Perform Audits"/>	

Item Counts	
Node Count:	1
Leaf Count:	1
Level Count:	2
Branch Count:	0

Figure 113: Tree Definition and Properties Page

8. Complete the fields as follows:

*Tree Name	Populated based on the search/create a new tree criteria.
*Structure ID	Enter the applicable information or select data by clicking the search icon.
*Effective Date	Enter the effective date or select a date from the calendar icon.
*Status	Defaults to Active . To change, select date from the drop-down list. Valid values are Active and Inactive .
*Description	Enter the description of the tree.
*Category	Enter the category or select data by clicking the search icon.
*Use of Levels	Defaults to Strictly Enforced . To change, select data from the drop-down list. Valid values are Level Not Used , Loosely Enforced , and Strictly Enforced .

Audits

All Detail Values in this Tree Check this box if applicable. This field is used for auditing purposes.

Allow Duplicate Detail Values Check this box if applicable. This field is used for auditing purposes.

Item Counts

Node Count Populated.

Leaf Count Populated.

Level Count Populated.

Branch Count Populated.

9. Click **OK**. The Enter Root Node for Tree page is displayed.

Enter Root Node for Tree

Tree Name: TEST

Step 1: Set Up Tree Levels

Level Name	All Values	Description	View Detail	Delete Level
	<input type="checkbox"/>		View Detail	Delete Level

Step 2: Define Root Node

*Root Node:

Figure 114: Enter Root Node for Tree Page

10. Complete the fields as follows:

Step 1. Set Up Tree Levels

Tree Levels

Level Name Click this field to sort the column.

All Values Check this box if applicable

Description Click this field to sort the column.

View Detail Click this field to sort the column

Delete Level Click this field to sort the column.

Step 2. Define Root Node

***Root Node** Enter the applicable abbreviated Root Node or select data by clicking the search icon.

11. Click **Add Level**. The Tree Levels page is displayed.

Tree Levels

Level Name: 

All Values

Figure 115: Tree Levels Page

12. Complete the fields as follows:

Level Name	Enter the Level Name or select data by clicking the search icon.
All Values	Populated with a check. Uncheck if applicable.

13. Click **Save** to save the information.

OR

Click **Close** to return to the Enter Root Node for Tree page.

Tree Viewer

The **Tree Viewer** option is used to view and print the tree.

To access the Tree Viewer option:

1. Select the **Tree Manager** menu group.
2. Select the **Tree Viewer** component. The Tree Viewer page - Find an Existing Value tab is displayed.

Tree Viewer

Enter any information you have and click Search. Leave fields blank for a list of all values.

Find an Existing Value

▼ Search Criteria

Search by:  begins with

Figure 116: Tree Viewer Page - Find an Existing Value Tab

3. Complete the fields as follows:

- Search by** Defaults to **Tree Name**. To change, select data from the drop-down list.
- begins with** Enter the data that corresponds to the search by field.

4. Click **Search**. The Tree Viewer page is displayed.

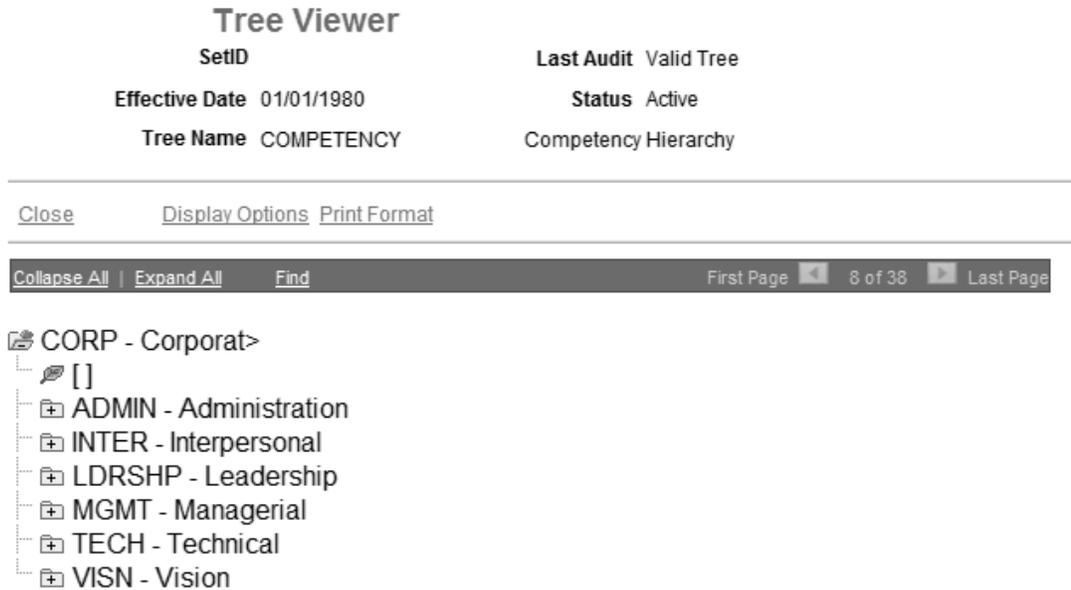


Figure 117: Tree Viewer Page

5. Complete the fields as follows:

- SetID** Populated from the search criteria entered.
- Last Audit** Populated.
- Effective Date** Populated with the current date.
- Status** Populated with the current status.
- Tree Name** Populated with the name of the tree.
- Collapse All** Allows the outline of the tree to collapse the folders.
- Expand All** Allows the outline of the tree to expand the folders.
- Find** Allows the user to search for a folder.

6. Click **Notify** to notify the next individual in the workflow.

Tree Auditor

The **Tree Auditor** option is used to find invalid or missing values.

To find/add a Tree Auditor:

1. Select the **Tree Manager** menu group.
2. Select the **Tree Auditor** component. The Audit Tree page - Find an Existing Value tab is displayed.

Audit Tree

Enter any information you have and click Search. Leave fields blank for a list of all values.

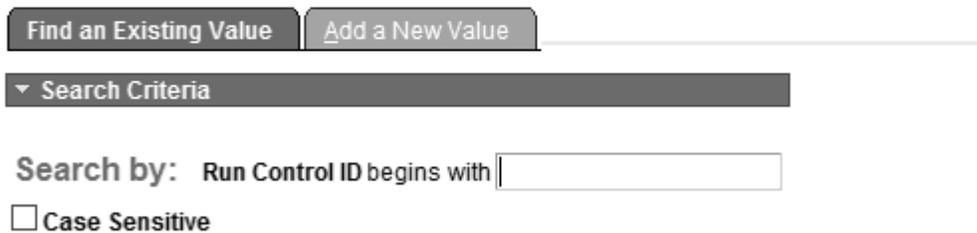


Figure 118: Audit Tree Page - Find an Existing Value Tab

3. Complete the fields as follows:

Search by: Run Control ID begins with Enter the run control ID.

Case Sensitive Check this box if the Run Control ID is case sensitive.

4. Click **Search**. The Tree Auditor page is displayed.

OR

Select the **Add a New Value** tab. The Audit Tree page - Add a New Value tab is displayed.

Audit Tree



Figure 119: Audit Tree Page - Add a New Value Tab

5. Complete the field as follows:

Run Control ID Enter the run control ID to be added.

6. Click **Add**. The Tree Auditor page is displayed.

Figure 120: Tree Auditor Page

7. Complete the fields as follows:

Run Control ID Populated from the search/add criteria entered.

Audit Scope

Single Tree Selected. Deselect if applicable.

Multiple Trees Select this field to select multiple trees.

Tree Definition

Tree Name Enter the tree name or select data by clicking the search icon.

SetId Enter the Set ID or select data by clicking the search icon. The search icon is displayed after a selection is made in the Tree Name field.

Date Selection

Effective Date of Tree Defaults to the current date. To change, select a date from the calendar icon.

As of Current Date Enter the as of current date or select a date from the calendar icon.

- As of Specific Date** Enter the as of specific date or select a date from the calendar icon.
- All Trees** Select this field for all trees.

8. Click **Save** to save the information. At this point, the following options are available:

Step	Description
Click Notify	Notifies the next individual.
Click Add	Returns to the Add a New Value tab.
Click Update Display	Updates the page.

Tree Structure

The **Tree Structure** option is used to add and update tree structure information.

To find/add a Tree Structure:

1. Select the **Tree Manager** menu group.
2. Select the **Tree Structure** component. The Tree Structure page - Find an Existing Tree Structure tab is displayed.

Tree Structure

Enter any information you have and click Search. Leave fields blank for a list of all values.



The screenshot shows a search interface with two tabs: "Find an Existing Tree Structure" (selected) and "Create New Tree Structure". Below the tabs is a "Search Criteria" dropdown menu. Underneath, there is a "Search by:" label followed by a dropdown menu currently set to "Tree Structure ID" and a "begins with" text box.

Figure 121: Tree Structure Page - Find an Existing Tree Structure Tab

3. Complete the fields as follows:

Search by Defaults to **Tree Structure ID**. To change, select data from the drop-down list. Valid values are **Description**, **Tree Structure ID**, and **Tree Structure Type**.

begins with Enter the data that corresponds with the search criteria entered.

4. Click **Search**. The Search Results page is displayed. This page displays a list of Tree Structure IDs, the Description of the Tree ID, and the Tree Structure Type.

OR

5. Select the **Create a New Tree Structure** tab. The Tree Structure page - Create a New Tree Structure tab is displayed.

Tree Structure

Find an Existing Tree Structure Create New Tree Structure

Tree Structure ID:

Figure 122: Tree Structure Page - Create New Tree Structure Tab

6. Complete the fields as follows:

Tree Structure ID Enter the applicable Tree Structure ID.

7. Click **Add**. The Tree Structure page - Structure tab is displayed.

Structure Levels Nodes Details

Tree Structure Properties

Structure ID: TEST

*Description:

*Type: Detail

Additional Key Field	Navigation Options
<input checked="" type="radio"/> SetId Indirection <input type="radio"/> Business Unit <input type="radio"/> User Defined <input type="radio"/> None	<input type="checkbox"/> Node Multi-Navigation <input type="checkbox"/> Detail Multi-Navigation

Figure 123: Tree Structure Page - Structure Tab

8. Complete the fields on the Tree Structure Properties page as follows:

Structure ID Populated based on the Tree Structure ID entered on the search/add criteria entered.

- *Description** Enter the description of the Structure ID.
- *Type** Defaults to **Detail**. To change, select data from the drop-down list. Valid values are **Detail** and **Summary**.
- Additional Key Field**
- SetId Indirection** Selected. Deselect if applicable. If this field is selected, do not select Business Unit, User Defined, or None.
- Business Unit** Select this field, if applicable. If this field is selected, do not select SetId Indirection, User Defined, or None.
- User Defined** Select this field, if applicable. If this field is selected, do not select SetId Indirection, Business Unit, or None.
- None** Select this field, if applicable. If this field is selected, do not select SetId Indirection, Business Unit, or User Defined.
- Navigation Options**
- Node Multi-Navigation** Select this field, if applicable.
- Detail Multi-Navigation** Select this field, if applicable.

9. Click **Save** to save the information. At this point, the following options are available:

Step	Description
Click Notify	Notifies the next individual.
Click Add	Returns to the Create New Tree Structure tab.
Click Update Display	Updates the page.

Tree Utilities

For more information see:

Copy/Delete Tree.....	113
Export Tree.....	115
Import Tree.....	117
Repair Tree.....	120
Repair Tree Reports.....	122

Copy/Delete Tree

The **Copy/Delete Tree** option is used to copy, delete, and audit a tree(s).

To copy/delete a tree:

1. Select the **Tree Manager** menu group.
2. Select the **Tree Utilities** menu.
3. Select the **Copy/Delete Tree** component. The Tree Maintenance page - Tree Maintenance tab is displayed.

Tree Maintenance Tree Structure Maintenance

Tree Maintenance

Tree Definitions					
Select	Key Type	User Key	Tree Name	Effective Date	Valid Tree
<input type="checkbox"/>	SetId	HXFRA	ALL_TIME	01/01/1901	Valid Tree
<input type="checkbox"/>	SetId	HXUSA	ALL_TIME	01/01/1901	Valid Tree
<input type="checkbox"/>	SetId	MBGEN	ALL_TIME	01/01/1901	Valid Tree
<input type="checkbox"/>	SetId	HXUSA	ALL_TIME_TC	01/01/2000	Valid Tree
<input type="checkbox"/>	SetId	MBGEN	ALL_TIME_TC	01/01/2000	Valid Tree
<input type="checkbox"/>	None		COMPETENCY	01/01/1980	Valid Tree
<input type="checkbox"/>	SetId	KPIND	DEPT_SECURITY	01/01/1979	Valid Tree
<input type="checkbox"/>	SetId	AUS01	DEPT_SECURITY	01/01/1980	Valid Tree
<input type="checkbox"/>	SetId	FRA01	DEPT_SECURITY	01/01/1980	Valid Tree
<input type="checkbox"/>	SetId	BNCAN	DEPT_SECURITY	01/01/1980	Valid Tree
<input type="checkbox"/>	SetId	BNUSA	DEPT_SECURITY	01/01/1980	Valid Tree
<input type="checkbox"/>	SetId	MBGEN	DEPT_SECURITY	01/01/1980	Valid Tree
<input type="checkbox"/>	SetId	BEL01	DEPT_SECURITY	01/01/1980	Valid Tree
<input type="checkbox"/>	SetId	KRSI1	DEPT_SECURITY	01/01/1980	Valid Tree
<input type="checkbox"/>	SetId	CAN01	DEPT_SECURITY	01/01/1980	Valid Tree

Figure 124: Tree Maintenance Page - Tree Maintenance Tab

4. Complete the fields as follows:

Tree Definitions

Select	Check this box to select the applicable line.
Key Type	Populated. Click this field to sort by Key Type.
User Key	Populated. Click this field to sort by User Key.
Tree Name	Populated. Click this field to sort by Tree Name.
Effective Date	Populated. Click this field to sort by Effective Date.
Valid Tree	Populated. Click this field to sort by Valid Tree.

- Select the **Tree Structure Maintenance** tab. The Structure Maintenance page - Tree Structure Maintenance tab is displayed.

Tree Maintenance		Tree Structure Maintenance		
Structure Maintenance				
Tree Structures				
Select	Tree Structure ID	Description	Node Record Name	Detail Record Name
<input type="checkbox"/>	ACAD_ORGANIZATION	Academic Organization	ACAD_ORG_TBL	SUBJECT_TBL
<input type="checkbox"/>	ALL_TIME_OLAP	All Time Tree for OLAP	TC_TREE_NODE	TC_ORG_VW
<input type="checkbox"/>	BUSINESS_UNIT	Business Unit	BUS_UNIT_TBL_HR	
<input type="checkbox"/>	COMPENSATION	Compensation Structure	TC_CATEGORY	TC_COMP_DEFN
<input type="checkbox"/>	COMPETENCY	Competency	CM_TYPE_TBL	COMPETENCY_TBL
<input type="checkbox"/>	DEPARTMENT	Department Security Chart	DEPT_TBL	
<input type="checkbox"/>	EQTN_ID_TREE	Equation ID Auth Structure	EQTN_IDAUTH_TBL	
<input type="checkbox"/>	EQTN_SQ_TREE	Equation SQL Tree	EQTN_SQAUTH_TBL	
<input type="checkbox"/>	EQTN_TB_TREE	Equation Data Tbl Tree Struct	EQTN_TBAUTH_TBL	
<input type="checkbox"/>	EQTN_XT_TREE	Equation Ext. Sub Auth Struct	EQTN_XTAUTH_TBL	
<input type="checkbox"/>	FA_ZIPCODE_REGIONS	Financial Aid Zip Code Regions	BDGT_REGION_TBL	RGN_POSTAL_TBL
<input type="checkbox"/>	GPFR_DADS	DADS	GPFR_DA_STR_VW	
<input type="checkbox"/>	ITEM_SECURITY	Item Security	TREE_NODE_TBL	ITEM_TYPE_TBL
<input type="checkbox"/>	OLAP_TIME	OLAP Time dimension	TREE_NODE_TBL	TC_OLAP_TIME
<input type="checkbox"/>	POSITION	Position Hierarchy	POSITION_DATA	
<input type="checkbox"/>	REGION	Recruiting Regions	REGION_TBL	RGN_POSTAL_TBL

Figure 125: Tree Maintenance Page - Tree Structure Maintenance Tab

- Complete the fields as follows:

Tree Structures

Select Check this box to select the applicable line.

Tree Structure ID Populated. Click this field to sort by Tree Structure ID.

Description Populated. Click this field to sort by Description.

Node Record Name Populated. Click this field to sort by Node Record Name.

Detail Record Name Populated. Click this field to sort by Detail Record Name.

At this point, the following options are available.

Step	Definition
Click Copy	Copies the tree.
Click Delete	Deletes the tree.

Click View	Displays the tree.
-------------------	--------------------

Export Tree

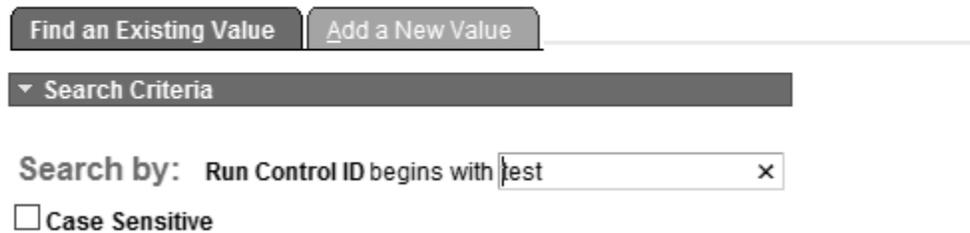
The **Export Tree** option is used to export a tree to a file.

To export a tree to a file:

1. Select the **Tree Manager** menu group.
2. Select the **Tree Utilities** menu.
3. Select the **Export Tree** component. The Export Tree page - Find an Existing Value tab is displayed.

Export Tree

Enter any information you have and click Search. Leave fields blank for a list of all values.



Find an Existing Value Add a New Value

▼ Search Criteria

Search by: Run Control ID begins with test x

Case Sensitive

Figure 126: Export Tree Page - Find an Existing Value Tab

4. Complete the fields as follows:

Search by: Run Control ID begins with Enter the Run Control ID.

Case Sensitive Check this box if the tree to be exported is case sensitive.

5. Click **Search**. The Tree Export page is displayed.

OR

Select the **Add a New Value** tab. The Export Tree page - Add a New Value tab is displayed.

Export Tree

Figure 127: Export Tree Page - Add a New Value Tab

- Complete the field as follows:

Run Control ID Enter the Run Control ID to be added.

- Click **Add**. The Tree Export page is displayed.

Tree Export

Figure 128: Tree Export Page

- Complete the fields as follows:

Run Control ID Populated from the search/add criteria entered.

***Output File Name** Enter the output file name.

Tree Definition

Tree Name Enter the tree name or select data by clicking the search icon.

Effective Date Enter the effective date or select a date from the calendar icon.

Tree Key Value	Enter the key tree name or select data by clicking the search icon.
Tree Data to Export	
Tree Definition	Populated.
Tree Structure	Check this box to select a tree structure.
Tree User Level	Check this box to select a tree user level.
Tree Level	Populated.
Tree Node/Leaf	Check this box to select a tree node/leaf.
Tree User Nodes	Check this box to select a tree user node.

9. Click **Save** to save the information. At this point, the following options are available:

Step	Description
Click Notify	Notifies the next individual.
Click Add	Returns to the Add a New Value tab.
Click Update Display	Updates the page.

Import Tree

The ***Import Tree*** option is used to import a tree from a flat file.

To Import a Tree:

1. Select the ***Tree Manager*** menu group.
2. Select the ***Tree Utilities*** menu.

3. Select the **Import Tree** component. The Import Tree page - Find an Existing Value tab is displayed.

Import Tree

Enter any information you have and click Search. Leave fields blank for a list of all values.

Find an Existing Value Add a New Value

▼ Search Criteria

Search by: Run Control ID begins with test x

Case Sensitive

Figure 129: Import Tree Page - Find an Existing Value Tab

4. Complete the fields as follows:

Search by: Run Control ID begins with Enter the Run Control ID.

Case Sensitive Click this box if the Role Name is case sensitive.

5. Complete the fields as follows:
6. Click **Search**. The Tree Import page is displayed.

OR

Select the **Add a New Value** tab. The Import Tree page - Add a New Value tab is displayed.

Import Tree

Find an Existing Value Add a New Value

Run Control ID: test x

Figure 130: Import Tree Page - Add a New Value Tab

7. Complete the fields as follows:

Run Control ID Enter the Run Control ID to be added.

8. Click **Add**. The Tree Import page is displayed.

Tree Import

Run Control ID: test [Report Manager](#) [Process Monitor](#)

*Input File Name

*Save Replace Tree if Exists Load Tree Defn from File

Tree Definition

Tree Name Effective Date

Structure All Values Allow Duplicate Leaf

SetId *Encoding

Description Category

Use Levels

Figure 131: Tree Import Page

9. Complete the fields as follows:

Run Control ID	Populated from the search/add criteria entered.
*Input File Name	Enter the input file name.
*Save Method	Defaults to Save . To change, select data from the drop-down list. Valid values are Saved and Save Draft .
Replace Tree if Exists	Checked and will replace an existing tree. Uncheck this box if applicable.
Load Tree Defn from File	Checked and will load the tree definition from a file. Uncheck this box if applicable.
Tree Definition	
Tree Name	Populated.
Effective Date	Populated.
Structure	Populated.
All Values	Populated.
Allow Duplicate Leaf	Populated.
SetId	Populated
Description	Populated.
Category	Populated.

Use Levels Populated. To change, select date from the drop-down list.

10. Click **Save** to save the information. At this point, the following options are available:

Step	Description
Click Notify	Notifies the next individual.
Click Add	Returns to the Add a New Value tab.
Click Update Display	Updates the page.

Repair Tree

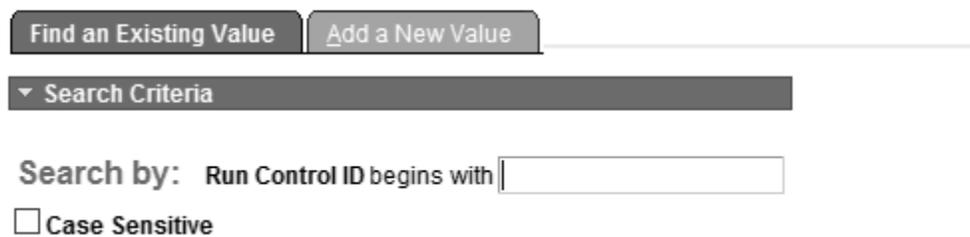
The **Repair Tree** option is used to audit and repair tree utilities.

To repair a tree:

1. Select the **Tree Manager** menu group.
2. Select the **Tree Utilities** menu.
3. Select the **Repair Tree** component. The Repair Trees page - Find an Existing Value tab is displayed.

Repair Trees

Enter any information you have and click Search. Leave fields blank for a list of all values.



Find an Existing Value Add a New Value

▼ Search Criteria

Search by: Run Control ID begins with

Case Sensitive

Figure 132: Repair Trees Page - Find an Existing Value Tab

4. Complete the fields as follows:

Search by: Run Control ID begins with Enter the Run Control ID.

Case Sensitive Click this box if the Role Name is case sensitive.

5. Click **Search**. The Repair Trees page is displayed.

OR

Select the **Add a New Value** tab. The Repair Trees page - Add a New Value tab is displayed.

Repair Trees



Find an Existing Value | **Add a New Value**

Run Control ID:

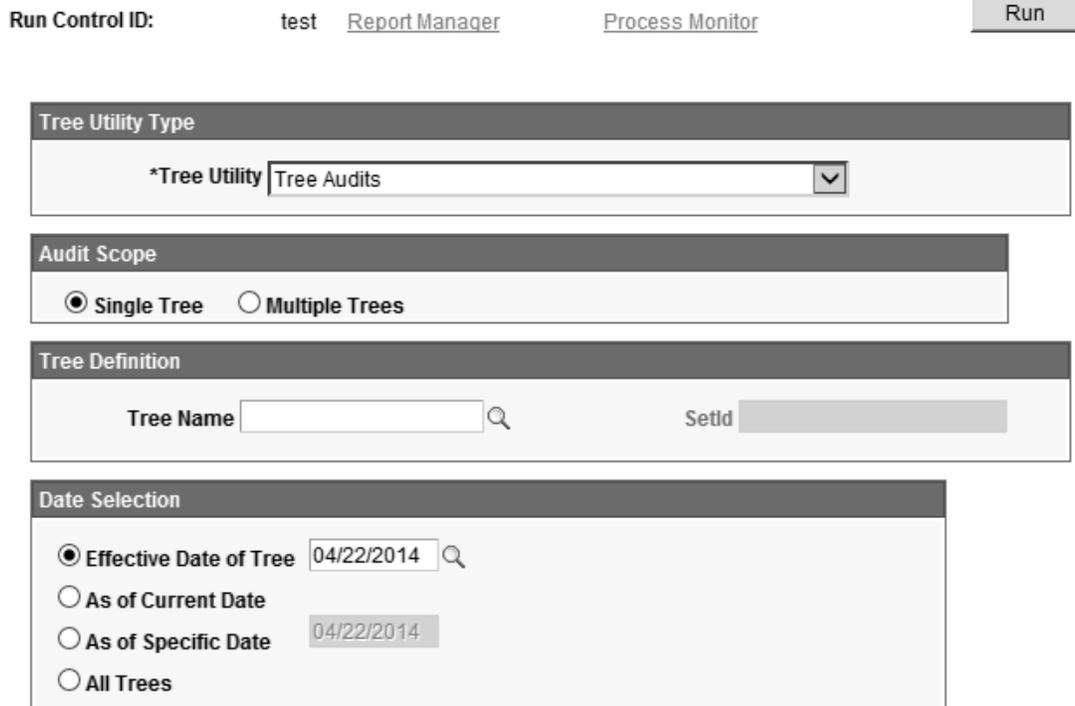
Figure 133: Repair Tree Page - Add a New Value Tab

6. Complete the fields as follows:

Run Control ID Enter the Run Control ID to be added.

7. Click **Add**. The Repair Tree page is displayed.

Repair Tree



Run Control ID: test [Report Manager](#) [Process Monitor](#) **Run**

Tree Utility Type

*Tree Utility ▼

Audit Scope

Single Tree **Multiple Trees**

Tree Definition

Tree Name 🔍 Setid

Date Selection

Effective Date of Tree 🔍

As of Current Date

As of Specific Date

All Trees

Figure 134: Repair Tree Page

8. Complete the fields on the Repair Tree page as follows:

Run Control ID	Populated with the search/add criteria entered.
Tree Utility Type	
*Tree Utility	Defaults to Tree Audits . To change, select data from the drop-down list.
Audit Scope	
Single Tree	Select this field if the audit is pertaining to a single tree.
Multiple Trees	Select this field if the audit is pertaining to multiple trees.
Tree Definition	
Tree Name	Enter the applicable tree name or select data by clicking the search icon.
SetId	Enter the applicable SetId.
Date Selection	
Effective Date of Tree	Populated with the current date. To change, select a date from the calendar icon.
As of Current Date	Select this field, if applicable.
As of Specific Date	Defaults to the current date. To change, select a date from the calendar icon.
All Trees	Select this field for all trees.

9. Click **Save** to save the information. At this point, the following options are available:

Step	Description
Click Notify	Notifies the next individual.
Click Add	Returns to the Add a New Value tab.
Click Update Display	Updates the page.

Repair Tree Reports

The ***Repair Tree Reports*** option is used to review results from the ***Repair Tree*** option.

To repair tree reports:

1. Select the ***Tree Manager*** menu group.
2. Select the ***Tree Utilities*** menu.

3. Select the **Repair Tree Reports** component. The Repair Tree Reports page - Find an Existing Value tab is displayed.

Repair Tree Reports

Enter any information you have and click Search. Leave fields blank for a list of all values.

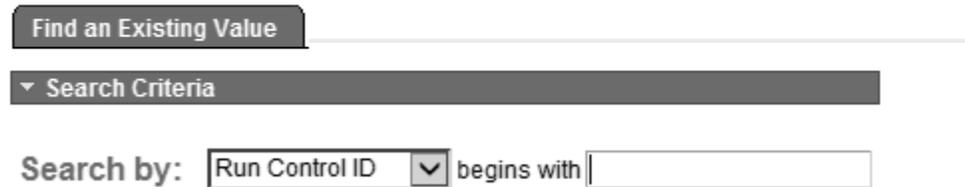


Figure 135: Repair Tree Reports Page - Find an Existing Value Tab

4. Complete the fields as follows:

Search by Defaults to **Run Control ID**. To change, select data from the drop-down list. Valid values are **Run Control ID** and **Process Instance**.

begins with Enter the data that corresponds to the search criteria entered.

5. Click **Search** to access the Repair Tree Reports.

Index

A

Assigning the Distributed Security Administrator Roles to a User • 13

C

Common Queries • 96

Copy Permission Lists • 57

Copy Roles • 70

Copy User Profiles • 24

Copy/Delete Tree • 113

Create and Maintain User Profiles • 16

Create New Oprid • 7

Creating a Distributed Security Administrator Role • 11

Creating a Row-Level Permission List • 6

D

Defining Roles That the Distributed Security Administrator Can Grant • 12

Delete Forgotten Password Hint • 80

Delete Permission Lists • 59

Delete Roles • 71

Delete User Profiles • 26

Digital Signature • 87

Distributed Security Administrator • 3

Distributed User Profiles • 27

Distributed User Set Up • 29

E

Employee Password Reset • 7

EmpowHR User Security (HD) • 1

Execute Role Rules • 73

Export Tree • 115

F

Forgotten Password Email Text • 77

Forgotten Password Hint • 79

G

Granting Roles and Row-Level Permission Lists • 4

I

Import Tree • 117

Introduction to Tree Manager • 102

M

Mass Change Operator Security • 97

P

Password Configuration • 73

Password Controls • 74

People Tools • 15

Permission Lists • 31

Permission Lists Overview • 8

Permissions and Roles • 31

Purge Inactive User Profiles • 29

Tree Auditor • 108

Tree Manager • 101

Tree Structure • 110

Tree Utilities • 112

Tree Viewer • 106

Q

Query Access List Cache • 95

Query Access Manager • 93

Query Security • 92

U

User Profile Types • 82

User Profiles • 9

User Profiles (People Tools) • 15

R

Repair Tree • 120

Repair Tree Reports • 122

Roles • 9

Roles Component • 60

S

Security Administrator Role • 11

Security Links • 85

Security Objects • 82

Signon PeopleCode • 91

Single Signon • 90

T

Tables to Skip • 84