

# NFC

## Procedures



**National Finance Center**  
Office of the Chief Financial Officer  
U.S. Department of Agriculture

June 2009

# *EmpowHR* – Version 9.0 Section 2 – User Security

TITLE I  
Payroll/Personnel Manual

CHAPTER 17  
EmpowHR

SECTION 2  
User Security

# Table Of Contents

<b><a href="#">EmpowHR User Security (HD)</a></b> .....	<b>1</b>
<a href="#">Security Administrator Role</a> .....	3
<a href="#">Creating A Distributed Security Administrator Role</a> .....	3
<a href="#">Defining Roles That The Distributed Security Administrator Can Grant</a> .....	5
<a href="#">Assigning The Distributed Security Administrator Roles To A User</a> .....	6
<a href="#">Distributed Security Administrator</a> .....	8
<a href="#">Granting Roles And Row-Level Permission Lists</a> .....	8
<a href="#">Creating A Row-Level Permission List</a> .....	11
<a href="#">Associating Department Security To New Row-Level Permission Lists</a> .....	13
<a href="#">Create New Oprid</a> .....	15
<a href="#">Employee Password Reset</a> .....	15
<a href="#">Permission Lists Overview</a> .....	15
<a href="#">Roles</a> .....	16
<a href="#">User Profiles</a> .....	17
<b><a href="#">People Tools</a></b> .....	<b>18</b>
<a href="#">User Profiles (People Tools)</a> .....	18
<a href="#">Create And Maintain User Profiles</a> .....	18
<a href="#">Copy User Profiles</a> .....	28
<a href="#">Delete User Profiles</a> .....	29
<a href="#">Distributed User Profiles</a> .....	31
<a href="#">Distributed User Set Up</a> .....	32
<a href="#">Purge Inactive User Profiles</a> .....	33
<a href="#">Permissions &amp; Roles</a> .....	34
<a href="#">Permission Lists</a> .....	34
<a href="#">Copy Permission Lists</a> .....	60
<a href="#">Delete Permission Lists</a> .....	61
<a href="#">Roles Component</a> .....	63
<a href="#">Copy Roles</a> .....	74
<a href="#">Delete Roles</a> .....	75
<a href="#">Execute Role Rules</a> .....	77
<a href="#">Password Configuration</a> .....	79
<a href="#">Password Controls</a> .....	79
<a href="#">Forgotten Password Email Text</a> .....	83
<a href="#">Forgotten Password Hint</a> .....	85
<a href="#">Delete Forgotten Password Hint</a> .....	87
<a href="#">Security Objects</a> .....	88
<a href="#">User Profile Types</a> .....	89
<a href="#">Tables To Skip</a> .....	91
<a href="#">Security Links</a> .....	91
<a href="#">Digital Signature</a> .....	95

<a href="#">Single Signon</a> .....	98
<a href="#">Signon Peoplecode</a> .....	99
<a href="#">Query Security</a> .....	100
<a href="#">Query Access Manager</a> .....	100
<a href="#">Query Access List Cache</a> .....	102
<a href="#">Common Queries</a> .....	103
<a href="#">Mass Change Operator Security</a> .....	103
<b><a href="#">Tree Manager</a></b> .....	<b>107</b>
<a href="#">Introduction To Tree Manager</a> .....	108
<a href="#">Tree Viewer</a> .....	113
<a href="#">Tree Auditor</a> .....	114
<a href="#">Tree Structure</a> .....	117
<a href="#">Tree Utilities</a> .....	119
<a href="#">Copy/Delete Tree</a> .....	119
<a href="#">Export Tree</a> .....	121
<a href="#">Import Tree</a> .....	124
<a href="#">Repair Tree</a> .....	126
<a href="#">Repair Tree Reports</a> .....	129
<a href="#">Heading Index</a> .....	<i>Index – 1</i>

## 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.

The *EmpowHR* application provides security features to ensure that 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. Group users 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 (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, TMGT, Table 5). 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* Department IDs are used in place of the NFC Organizational Codes and are required for various types of transactions within the application. Prior to data being loaded into the *EmpowHR* application, these IDs must be established in order to translate each unique NFC Organizational Code for organizations into unique *EmpowHR* department IDs (DEPTID).

Also, prior to the agency data being loaded into the *EmpowHR* application and based on information the agency provided, a security tree is created that represents the agency's organization's 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 is 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 considerable increases the number of potential users the system must accommodate, an efficient method of granting authorization to varying user types is needed. Security definitions provide a modular means to apply security attributes in a scalable manner.

Each user of the system 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 exception to this rule. The following table provides a summary of each profile and the description of each:

User	Description
Super User	Considered the application expert, this user understand the setup of the application and has access to the define business rules area for the application. In addition, they have full access to all data entry pages, correction mode capabilities to modify historical data, and are able to run all processes within their application.
Lead User	This user type has full access to all data entry pages, correction mode capabilities to modify historical data, and is able 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 user that perform tasks such as approving, data entry, updating existing data, and processing.
Data Entry	This user has access to a very limited number of pages within an 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 to to the restrictiveness.
Inquiry	These users have access to some pages of the application in a ready 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, running processes, system. access, User IDs, and sign-on and time-out 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 can not conduct transactions for. Access is limited via business unit and department role.
Inquiry	Security set-up through departmental roles to allow read only access to certain data entry or transaction pages and online inquiry pages with predefined search capabilities. <b>EmpowHR</b> Query toll allow security control at table level security, row level security, field level security , and run only.
Transaction Processing	Data entry and transaction processing limited by assigning security based on user roles in the <b>EmpowHR</b> application. 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 funning certain processes.
External Process	Users gain access to the application remotely via the internet with appropriate authentication.
User ID	Security configuration to allow users the ability to access applications and be able to move tween them without having to log in and out.

Component	Security Description
Sign-on Time	Adjustable interval during which a user is allowed to access the application or sign onto <b>EmpowHR</b> .
Time-out	Specifies the amount of time the user's machine can remain idle before <b>EmpowHR</b> automatically disconnects the user from the application so they could not gain access.

Below is a brief description of the various roles and steps that are performed by the Security Administrator and the Distributed Security Administrator.

This section contains the following topics:

[Security Administrator Role](#)

[Distributed Administrator Role](#)

This section also contains a detailed explanation of each component.

[Create New Oprid](#)

[Employee Password Reset](#)

[Permission Lists](#)

[Roles](#)

[User Profiles](#)

## Security Administrator Role

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

This section contains the following topics:

[Creating A Distributed Security Administrator Role](#)

[Defining Roles That The Distributed Security Administrator Can Grant](#)

[Assigning The Distributed Security Administrator Roles To A User](#)

### ***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 (Sub-Agency 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 Add A New Value tab - Roles page (**Figure 1**) is displayed.

The screenshot shows the 'Roles' page with two tabs: 'Find an Existing Value' and 'Add a New Value'. The 'Add a New Value' tab is active. Below the tabs, there is a 'Role Name:' label followed by an empty text input field. Below the input field is a yellow 'Add' button. At the bottom of the page, there are two links: 'Find an Existing Value' and 'Add a New Value'.

Figure 1. Add A New Value tab - Roles page

5. Enter the Role Name.
6. Click **Add**. The General tab - Role page(Figure 2) is displayed.

The screenshot shows the 'General' tab of the 'Role' page. The 'Role Name' field is populated with 'NFC Remote Security Admin'. Below it is a 'Description:' label followed by an empty text input field. Below the description field is a 'Long Description' section with a large empty text area. At the bottom of the page, there are three buttons: 'Save', 'Add', and 'Update/Display'. Below the buttons is a navigation bar with links: 'General | Permission Lists | Members | Dynamic Members | Workflow | Role Grant | Links | Role Queries | Audit'.

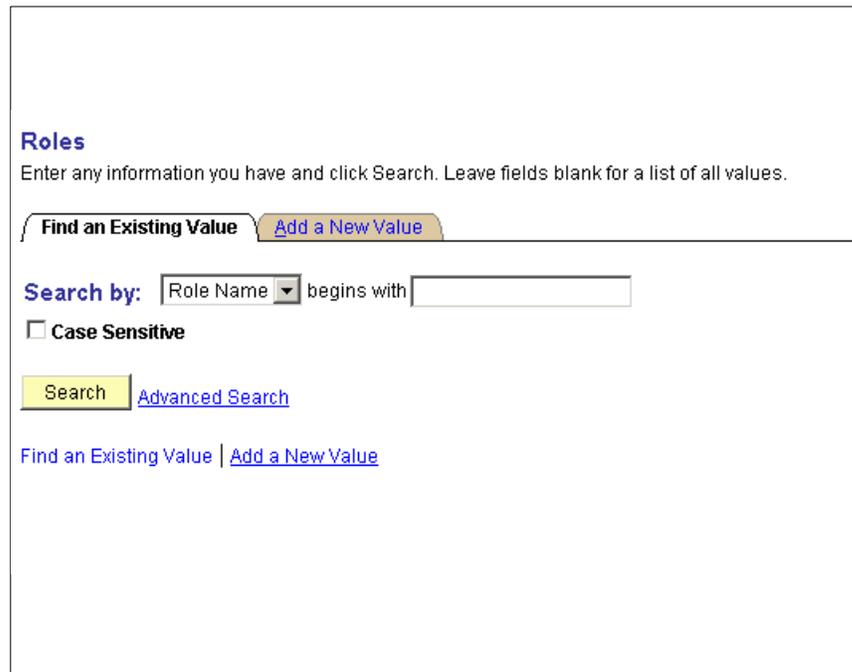
Figure 2. General tab - Role page

7. Enter the description of the role.
8. 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 grant.

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 Find An Existing Value tab - Roles page(**Figure 3**) is displayed.



**Roles**  
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 by: Role Name begins with

Case Sensitive

Search | [Advanced Search](#)

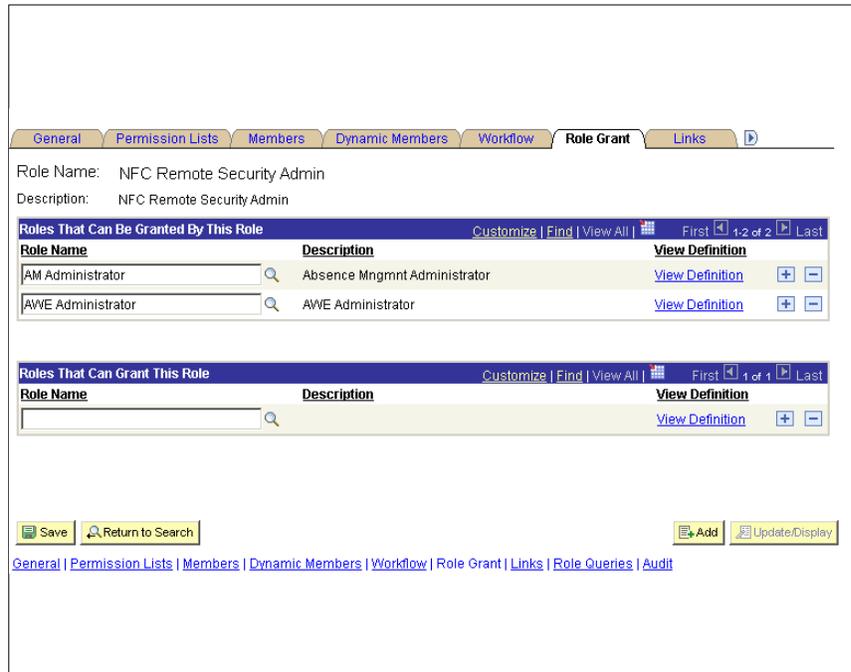
[Find an Existing Value](#) | [Add a New Value](#)

**Figure 3. Find An Existing Value tab - Roles page**

5. Select **Description** or **Role Name** from the drop-down list.
6. Enter all, or part of the Description or Role Name based on the selection from the drop-down list.

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

7. Click **Search**.
8. Select a value.
9. Select the Role Grant tab. The Role Grant tab - Roles page(**Figure 4**) is displayed.



**Figure 4. Role Grant tab - Roles page**

10. Enter the Role Name in the Roles That Can Be Granted By This Role section, then click the lookup icon.
11. Click **Search**.
12. Select a value.
13. Click **Save**.

**Note:** Click 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 Find An Existing Value tab - User Profiles page(**Figure 5**) is displayed.

**User Profiles**  
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 by:**  begins with

[Search](#) [Advanced Search](#)

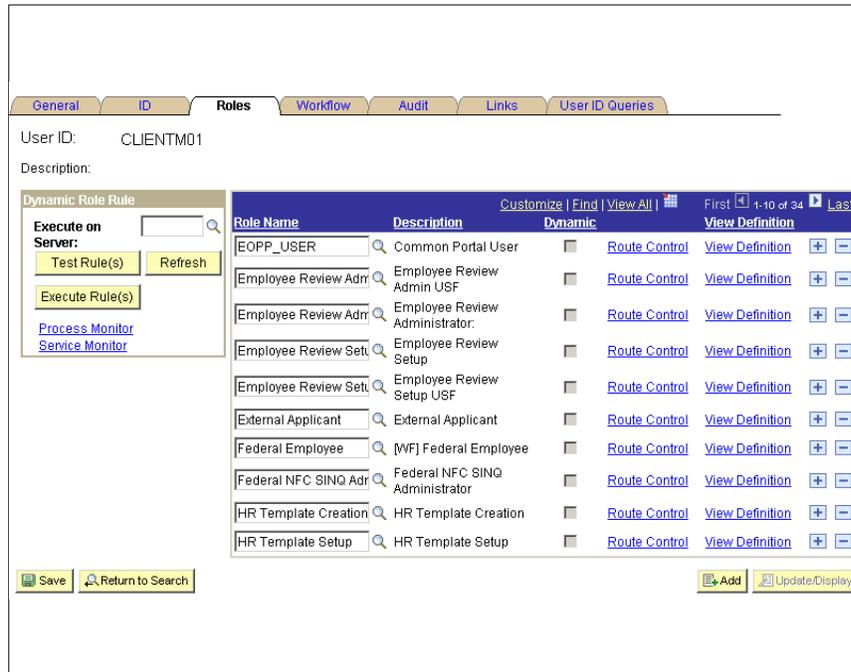
[Find an Existing Value](#) | [Add a New Value](#)

**Figure 5. Find An Existing Value tab - User Profiles page**

5. Select **Description** or **User ID** from the drop-down list.
6. Enter all or part of the Description or User ID.
7. Select the Role Name from the look up results.

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

8. Click **Search**.
9. Select the Roles tab. The Roles tab - User Profiles page(**Figure 6**) is displayed.



**Figure 6. Roles tab - User Profiles page**

10. Click **Add** to add a new row.
11. Click the lookup icon.
12. Select the Role Name from the look up results.
13. Click **Save**.

## Distributed Security Administrator

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

This section contains the following topics:

[Granting Roles And Row-Level Permission Lists](#)

[Creating A Row-Level Permission List](#)

[Associating Department Security To New Row-Level Permission List](#)

[Assigning Department Security To A Permission List](#)

### **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 Find An Existing Value tab - Distributed User Profile page(**Figure 7**) 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 by:** User ID  begins with

**Search** [Advanced Search](#)

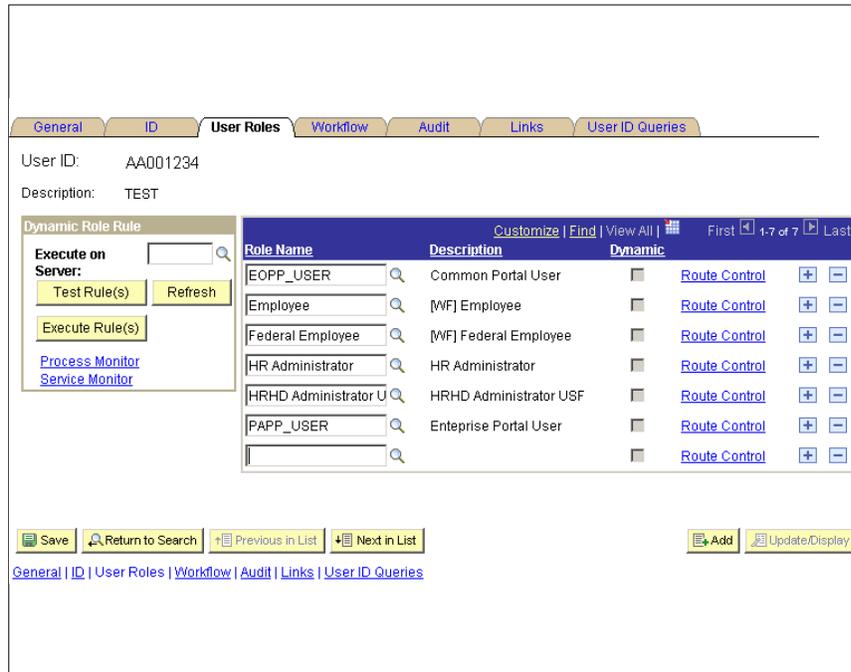
[Find an Existing Value](#) | [Add a New Value](#)

**Figure 7. Find An Existing Value tab - Distributed User Profiles page**

5. Select **Description** or **User ID** from the drop-down list.
6. Enter all or part of the Description or User ID.

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

7. Click **Search**.
8. Select a Role Name from the search criteria.
9. Select the User Roles tab. The User Roles tab - Distribute User Profiles page(**Figure8**) is displayed.



**Figure 8. User Roles tab - Distributed User Profiles page**

10. Click + to add an additional Role.
11. Click the lookup 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.
12. Select the applicable Role Name.
13. Click **Save**.
14. Click the General tab. The General tab - Distributed User Profiles page(**Figure 9**) is displayed.

The screenshot displays the 'General' tab of a user profile in EmpowHR. At the top, there are tabs for 'General', 'ID', 'User Roles', 'Workflow', 'Audit', 'Links', and 'User ID Queries'. The 'General' tab is active. The user ID is 'AA001234' and the description is 'TEST'. There is a checkbox for 'Account Locked Out?'. The 'Logon Information' section includes a dropdown for 'Symbolic ID' (sa1), password fields, a 'Password Expired?' checkbox, and a 'User ID Alias' field. Below this is the 'General Attributes' section with dropdowns for 'Language Code' (English) and 'Currency Code' (US Dollar), and a checkbox for 'Enable Expert Entry'. The 'Default Mobile Page' field has a search icon. The 'Permission Lists' section contains four fields: 'Navigator' (HCSPNAVHP), 'Homepage' (HCCPFGALLP), 'Process Profile' (HCCPFGALLP), 'Primary' (HCPPFED), and 'Row Security' (EMPOWHR), each with a search icon and an 'Explain' link. At the bottom, there are buttons for 'Save', 'Return to Search', 'Previous in List', 'Next in List', 'Add', and 'Update/Display'. A breadcrumb trail at the bottom reads 'General | ID | User Roles | Workflow | Audit | Links | User ID Queries'.

Figure 9. General tab - Distributed User Profiles page

15. Click the lookup icon next to the Row Security field to display Permission List(s).
16. Select the applicable Permission List. This field grants access to the user ID in order to view data in a component within the application.
17. 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 Find An Existing Value tab - Permission List page (Figure 10) is displayed.

The screenshot shows the 'Permission Lists' section of a web application. At the top, there is a heading 'Permission Lists' followed by the instruction 'Enter any information you have and click Search. Leave fields blank for a list of all values.' Below this, there are two tabs: 'Find an Existing Value' (which is active) and 'Add a New Value'. Under the active tab, there is a search interface. It starts with 'Search by:' followed by a dropdown menu currently set to 'Permission List' and a text input field labeled 'begins with'. Below the search fields are two buttons: 'Search' and 'Advanced Search'. At the bottom of the search area, there are two links: 'Find an Existing Value' and 'Add a New Value'.

**Figure 10. Find An Existing Value tab - Permission Lists page**

5. Select the Add A New Value tab. The Add A New Value tab - Permission List page(**Figure 11**) is displayed.

The screenshot shows the 'Add A New Value' tab on the 'Permission Lists' page. The heading 'Permission Lists' is at the top. Below it, there are two tabs: 'Find an Existing Value' and 'Add a New Value' (which is active). Under the active tab, there is a form with a label 'Permission List:' followed by a text input field containing the text 'HR'. Below the input field is a yellow 'Add' button. At the bottom of the form area, there are two links: 'Find an Existing Value' and 'Add a New Value'.

**Figure 11. Add A New Value tab - Permission List page**

6. Enter the name of the new permission list.
7. Click **Add**.

The screenshot shows the 'General' tab of the 'Permission Lists' page. At the top, there are navigation tabs: 'General', 'Pages', 'PeopleTools', 'Process', and 'Sign-on Times'. Below the tabs, the 'Permission List' is set to 'HR'. There is a 'Description' field. A section titled 'Permission List General' contains a 'Navigator Homepage' field with a search icon, and two checkboxes: 'Can Start Application Server?' and 'Allow Password to be Emailed?'. Another section titled 'Time-out Minutes' has two radio button options: 'Never Time-out' (which is selected) and 'Specific Time-out (minutes)' with an empty input field. At the bottom, there are three buttons: 'Save', 'Add', and 'Update/Display'.

Figure 12. General tab - Permission Lists page

8. Click **Save**.

### ***Associating Department Security To New Row-Level Permission Lists***

Below is the step-by-step process that will allow the Security Administrator to associate the Department Tree Security to the new Row-Level Permission List.

1. Select the ***Set Up HRMS*** menu group.
2. Select the ***Security*** menu.
3. Select the ***Core Row Level Security*** menu item.
4. Select the ***Security By Dept Tree*** component. The Find An Existing Value tab - Setup Dept Security Tree Acc. page is displayed.
5. Select the Add A New Value tab. The Add A New Value tab- Setup Dept Security Tree Acc. page (**Figure 13**) is displayed.



Figure 13. Add A Value tab - Setup Dept Security Tree Acc. page

6. Click the look-up to display the Row Security Permission List.
7. Select the applicable Permission List.
8. Click **Add**. The Security By Dept tab page (**Figure 14**) is displayed.

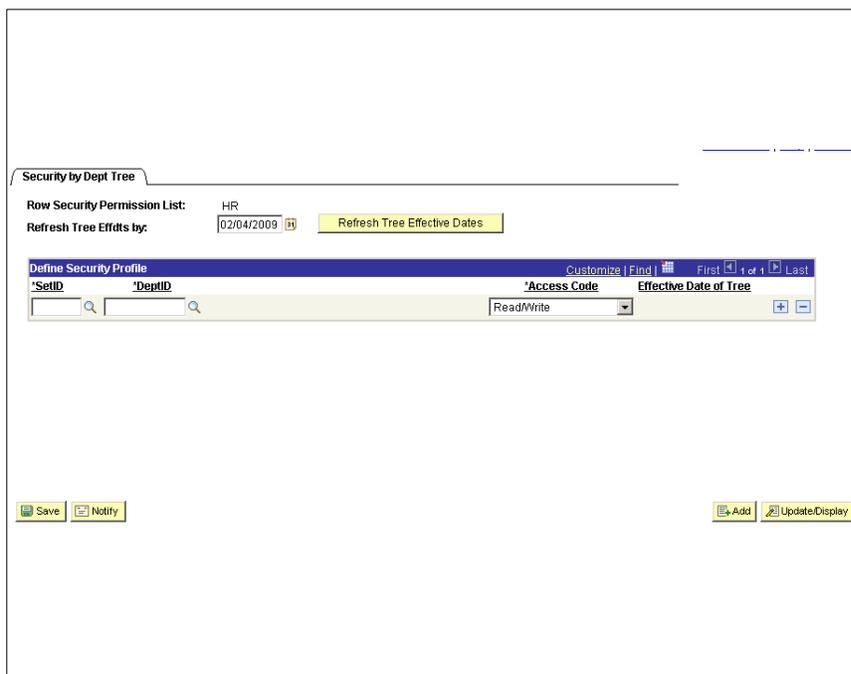


Figure 14. Security By Dept Tree tab - Security By Dept Tree page

9. Click the look-up for the Set ID. Select the applicable Set ID.

10. Click the look-up for the Department ID. Select the applicable Department ID.
11. Click **Save**.

## 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 re-routed 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 in this procedure.

## 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 re-routed 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 in this procedure.

## 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 agcy will use them with. Recall that roles are intermediary objects between permission lists and users. The agency uses roles to assign application permissions to users automatically.

Application Permission lists may contain a variety of accessibility, such as 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.

The **EmpowHR** application enforces data permission security with security search views. To understand how this is done, it helps to understand how the system retrieves data when the

user accesses a menu selection. When the user opens a menu selection in *EmpowHR*, the system displays a search page. 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. The system uses the information that the user enters in a key or altering key fields to select the box of data that the user wants to view or manipulate. A search page may have EmplID as a key field and Name as an alternate key. If the user enters Smith in the Name field, the system retrieves all the data rows with the Name field data that matches Smith. the system 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. The system 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, to the SQL (Structured Query Language) select statement along with the values that the user entered on the search page. The system retrieves the data that matches the criteria from the search page and the user's data Row-Level security permission List. The system doesn't retrieve data for people to whom you haven't 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. SETID's, associated DEPTID's, and Access Codes are what set apart a Row-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-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 the *Permission Lists*.

**Note:** When the *Permission Lists* component is selected from the *EmpowHR User Security (HD)* menu group, the user is re-routed 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 in this procedure.

## 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 the *EmpowHR* application.

This option is used to create and maintain roles established in the database. For more information about Roles, refer to People Tools, Roles 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 re-routed 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** section, [Roles](#) topic in this procedure.

## 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 inherited from the linked roles.

It is possible to have a user profile with no roles. This might be a user who isn't allowed access to the **EmpowHR** application; 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 re-routed 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 the **People Tools** section, [User Profiles](#) topic in this procedure.

## People Tools

This section contains the following topics:

[User Profiles](#)

[Permissions & Roles](#)

[Password Configuration](#)

[Security Objects](#)

[Query Security](#)

[Common Queries](#)

[Mass Change Operator Security](#)

### User Profiles (People Tools)

User profiles define the individual *EmpowHR* users access. The agency defines user profiles and then links them to one or more roles. A users profiles must be linked to at least one roles in order to be a valid profile. The majority of values that make up a user profiles are inherited form 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 a users, such as a user password, an email address, a Row-Security Permission List, and employee ID, and so on.

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 from this option.

This section contains the following topics:

[Create And Maintain User Profiles](#)

[Copy User Profiles](#)

[Delete User Profiles](#)

[Distribute User Profiles](#)

[Distributed User Set Up](#)

[Purge Inactive User Profiles](#)

#### **Create And Maintain User Profiles**

**To Create and Maintain User Profiles:**

1. Select *People Tools* menu group.
2. Select *User Profiles* component. The Find An Existing Value tab - User Profiles page (**Figure 15**) is displayed.

**Figure 15. Find An Existing Value tab - User Profiles page**

3. Complete the fields as follows:

**Search By** Click the down arrow and make the applicable selection. This field defaults to **Role Name**. Valid values are **Role Name, Description**.

**Begins With** Enter the applicable information.

4. Click **Search**. The General tab - User Profiles page (**Figure 17**) is displayed.

**OR**

Click **Add A New Value** tab. The Add A New Value tab - User Profiles page (**Figure 16**) is displayed. Click **Add**. The General Tab - User Profiles page(**Figure 17**) is displayed.

**Figure 16. Add A New Value tab - User Profiles page**

5. 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. If the user attempts to put spaces in the User ID, an error message will display.

Figure 17. General tab - User Profiles page

6. Complete the fields as follows:

**User ID** This field is populated based on the User ID entered on the Add A New Value tab - User Profiles page (Figure 16).

**Description** This field is populated based on the Description entered on the Add A New Value tab - User Profiles page (Figure 16).

**Account Locked Out?** Click this field to lock out a user’s account.

**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.

**Language Code** This field defaults to **English**. To change, select data from the drop-down list. The valid values are as follows:

Language Code
Arabic
Can French

Language Code
Czech
Danish
Dutch
English
French
Finnish
German
Greek
Hebrew
Hungarian
Italian
Japanese
Korean
Malay
Norwegian
Polish
Portuguese
Russian
S Chinese
Spanish
Swedish
T Chinese
Thai
Turkish

- Enable Expert Entry**      Click this field to enable expert entry.
  
- Currency Code**      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 search icon.
  
- Navigator Homepage**      This field is populated and cannot be changed.
  
- Primary**      This field is populated based on the Description entered on the Add A New Value tab - User Profiles page (**Figure 16**).
  
- Process Profile**      This field is populated and cannot be changed.
  
- Row Security**      Enter the applicable position name or select data by clicking search icon.

7. Click the **Edit Email Addresses** link to add or modify email addresses if applicable.
8. Click the **ID** tab. The ID tab - User Profiles page (**Figure 18**) is displayed.

The screenshot shows the 'ID' tab of the 'User Profiles' page. At the top, there are navigation tabs: General, ID (selected), Roles, Workflow, Audit, Links, and User ID Queries. Below the tabs, the 'User ID' is 'user1' and the 'Description' field is empty. A section titled 'ID Types and Values' contains a dropdown menu for 'ID Type' and a table with columns 'Attribute Name', 'Attribute Value', and 'Description'. Below this is a 'User Description' section with a 'Description' field and a 'Set Description' link. At the bottom, there are 'Save', 'Add', and 'Update/Display' buttons, along with a breadcrumb trail: General | ID | Roles | Workflow | Audit | Links | User ID Queries.

**Figure 18. ID tab - User Profiles page**

9. Complete the fields as follows:

**User ID** This field is populated based on the search/add criteria.

**Description** This field is populated based on the search/add criteria.

**ID Type** Click the down arrow to select the ID Type. The valid values are **Employee** and **None**.

**Attribute Name** This field is populated with the EmpIID if **Employee** is selected in the ID Type field. If the ID. 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** This field is populated. Click the link to sort this list by Description.

**Description** Enter the user description in this field.

10. Select **Roles**. The Roles tab - User Profiles page (**Figure 19**) is displayed.

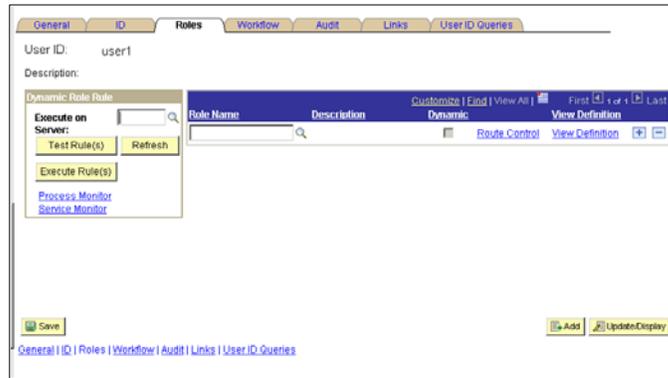


Figure 19. Roles tab - User Profiles page

11. Complete the fields as follows:

- |                          |   |
|--------------------------|---|
| <b>User ID</b>           | This field is populated based on the search/add criteria.   |
| <b>Description</b>       | This field is populated based on the search/add criteria  |
| <b>Execute On Server</b> | Enter the server name or select data by clicking the search icon.   |
| <b>Role Name</b>         | Enter the applicable role or select data by clicking the search icon. Click the link to sort the list by Role Name.           |
| <b>Description</b>       | This field is populated based on the role enter or selected in the Role Name. Click the link to sort the list by Description. |
| <b>Dynamic</b>           | Check is box if applicable. Click the link to sort the list by Dynamic.   |

12. Click the **Route Control** link. The User Route Control Profiles page (**Figure 20**) is displayed.

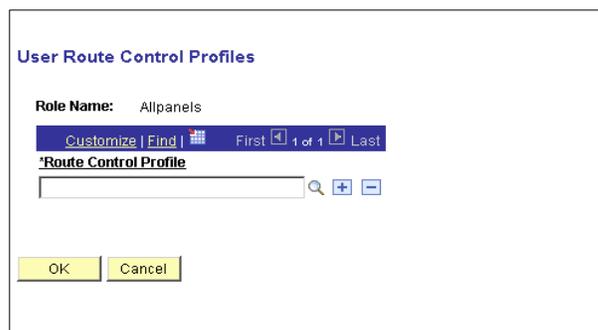


Figure 20. User Route Control Profiles page

**Role Name** This field is populated.

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

13. Click **OK**.

**OR**

Click **Cancel** to return to the Roles tab - User Profiles page (**Figure 19**).

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

15. Select **Workflow**. The Workflow tab - User Profiles page (**Figure 21**) 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 forward new worklist items to the alternate user one the profile is saved, if the From and To date range is completed. **Note:** It does not reassign items already in the user’s worklist.
- 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 worklist 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 worklist entries to the specified user and the Total pending Worklist 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 worklist or to an email mailbox. If the user doesn’t have access to one or both of these places, clear the check box.

**Figure 21. Workflow tab - User Profiles page**

16. Complete the fields as follows:

**User ID** This field is populated based on the User ID used in the search/add criteria.

<b>Description</b>	This field is populated based on the Description used in the search/add criteria.
<b>Alternate User ID</b>	Enter the alternate user ID for a user or select data from the drop-down list.
<b>Worklist User</b>	Check this box if the user is a worklist user.
<b>Email User</b>	Check this box if the user is an e-mail user.
<b>From Date</b>	Enter the from date in <b>MM/DD/YYYY</b> format or select a date from the calendar icon.
<b>To Date</b>	Enter the to date in <b>MM/DD/YYYY</b> format or click the icon to select a date from the calendar icon.
<b>Reassign Work To</b>	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.
<b>Total Pending Worklist Entries</b>	This field is populated with the number of pending worklist entries.

17. Select **Audit**. The Audit tab - User Profiles page (**Figure 22**) is displayed. The Audit page is a display only pages that enables the Administrator to determine when a profile was last updated and/or who updated the profile.



**Figure 22. Audit tab - User Profiles page**

18. Complete the fields as follows:

<b>User ID</b>	This field is populated based on the User ID entered on the search/add criteria.
----------------	--

**Description** This field is populated based on the Description entered on the search/add criteria.

**Last Update User ID** This field is populated.

**Last Update Date/Time** This field is populated.

19. Select **Links**. The Links tab - User Profiles page (**Figure 23**) is displayed.



**Figure 23. Links tab - User Profiles page**

20. Complete the fields as follows:

**User ID** This field is populated based on the User ID entered on the search/add criteria.

**Description** This field is populated based on the Description entered on the search/add criteria.

**Description** Check this box to sort the list by Description.

21. Select the **User ID Queries** tab. The User ID Queries tab - User Profiles page (**Figure 24**) is displayed.

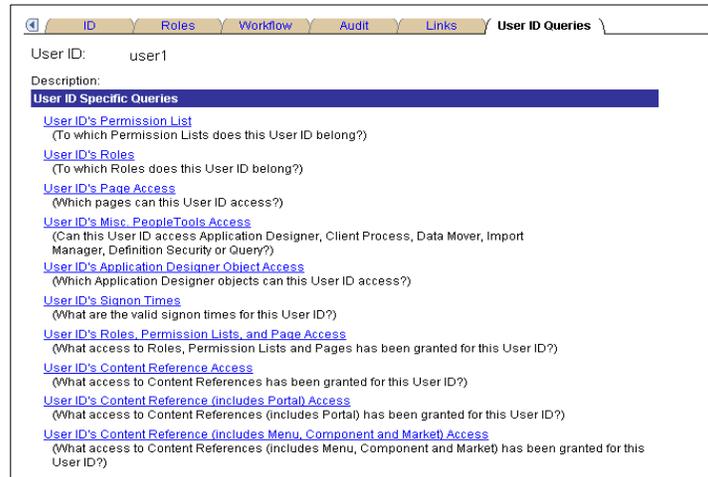


Figure 24. User ID Queries tab - User Profiles page

22. Complete the fields as follows:

**User ID** This field is populated based on the User ID.

**Description** This field is populated based on the Description entered on the search/add criteria.

**User ID Specific Queries** This field displays a list of the following links:

- The **User ID's Permission List** link to view which Permission Lists are associated with a User ID.
- The **User ID's Roles** link displays which roles are associated with a User ID.
- The **User ID's Page Access** link displays a list of which pages a user can access.
- The **User ID's Misc. People Tools Access** link displays which a user can access Application Designer, Client Process, Data Mover, Import Manager, Definition Security, or Query.
- The **User ID's Application Designer Object Access** link displays which Application Designer objects the user can access.
- The **User ID's Signon Times** link displays the valid signon times for the User ID.
- The **User ID's Roles, Permission Lists, And Page Access** link displays which roles, permission lists, and pages the User ID has access to.
- The **User ID's Content Reference Access** link displays which content references this User ID has been granted access.
- The **User ID's Content Reference (Includes Portal) Access** link displays which content references (including portal) this User ID has been granted access.
- The **User ID's Content Reference (Includes Menu, Component, And Market) Access** link displays which content references (including menu, component, and market) this User ID has been granted access.

- The **User ID's Content Reference (Includes Portal, Menu, Component, And Market) Access** link displays which content references (including portal, menu, component, and market) this User ID has been granted access.
- The **User ID's Web Service Operation Access** link displays which access to Web Service Operation has been granted for this User ID.

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

Step	Description
Click <b>Add</b>	To return to the Add A New Value tab.
Click <b>Update/Display</b>	To return 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 Find An Existing Value tab - Copy User Profiles page (**Figure 25**) is displayed.

**Figure 25. Find An Existing Value tab - Copy User Profiles page**

4. Complete the fields as follows:

**Search By** This field defaults to **User ID**. To change, select data from the drop-down list. The valid values are **User ID** and **Description**.

**Begins With** Enter the information that corresponds to the search by value.

**Case Sensitive** Check this box if the user profile is case sensitive.

5. Click **Search**. The Copy User Profiles page (**Figure 26**) is displayed.

**Figure 26. Copy User Profiles page**

6. Complete the fields as follows:

**\*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** Re-enter 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 General Tab - User Profiles page (**Figure 17**) is displayed. At this point, the following options are available:

Step	Description
Click <b>Return To Search</b>	The Find An Existing Value tab - Copy User Profiles page ( <b>Figure 25</b> ) is displayed.
Click <b>Refresh</b>	To refresh the page.

### Delete User Profiles

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

**To delete a user profile:**

1. Select the **People Tools** menu group.
2. Select the **User Profiles** menu.
3. Select the **Delete User Profiles** component. The Find An Existing Value tab - Delete User Profile page (**Figure 27**) is displayed.

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

**Find an Existing Value**

**Search by:** User ID begins with

Case Sensitive

[Advanced Search](#)

**Figure 27. Find An Existing Value tab - Delete User Profiles page**

4. Complete the fields as follows:

**Search By** This field defaults to **User ID**. To change, select data from the drop-down list. The valid values are **User ID** and **Description**.

**Begins With** Enter the applicable information.

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

5. Click **Search**. The Delete User Profile page (**Figure 28**) is displayed.

**Delete User Profile**

**User ID:** AA002924  
**Name:** Anderson, Annemarie  
**EmpID:** 002924

**Figure 28. Delete User Profile page**

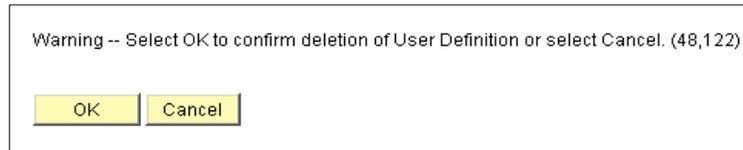
6. Complete the fields as follows:

**User ID** This field is populated based on the search/add criteria.

**Begins With** This field is populated with the corresponding search/add criteria entered.

**Case Sensitive** Check this box if the search/add criteria is case sensitive.

7. Click **Delete User Profile**. The User Profile Delete Confirmation pop-up (**Figure 29**) is displayed.



**Figure 29. User Profile Delete Confirmation pop-up**

8. Click **OK** to delete the permissions list and return to the Find An Existing Value tab - Delete User Profiles page (**Figure 27**).

**OR**

Click **Cancel** to cancel the deletion and return to the Find An Existing Value tab - Delete User Profiles page (**Figure 27**).

### ***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 Find An Existing Value tab - Distributed User Profiles page (**Figure 30**) is displayed.



**Figure 30. Find An Existing Value tab - Distributed User Profiles page**

4. Complete the fields as follows:

**Search By**

This field defaults to **User ID**. To change, select data from the drop-down list. The valid values are **User ID** and **Description**.

**Begins With**

Enter the applicable information that corresponds to the search by criteria.

5. Click **Search**. The General tab - User Profiles page (**Figure 17**) is displayed.

**OR**

Click the **Add A New Value** tab. The Add A New Value tab - Distributed User Profiles page (**Figure 31**) is displayed.



**Figure 31. Add A New Value tab - Distributed User Profiles page**

6. Complete the User ID field as follows:

<b>User ID</b>	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 General Tab - User Profiles page (**Figure 17**) 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 (**Figure 32**) is displayed.



**Figure 32. Set Distributed User Profile Search Record page**

4. Complete the field as follows:

<b>New Search Record</b>	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 Find An Existing Value tab - Purge Inactive User Profiles page (**Figure 33**) is displayed.

The screenshot shows the 'Purge Inactive User Profiles' page with the 'Find An Existing Value' tab selected. The page title is 'Purge Inactive User Profiles' and it includes the instruction: 'Enter any information you have and click Search. Leave fields blank for a list of all values.' There are two tabs: 'Find an Existing Value' (active) and 'Add a New Value'. Below the tabs is a search field with the label 'Search by: Run Control ID begins with'. There is a checkbox for 'Case Sensitive'. Below the search field are two buttons: 'Search' and 'Advanced Search'. At the bottom, there are links for 'Find an Existing Value' and 'Add a New Value'.

**Figure 33. Find An Existing Value tab - Purge Inactive User Profiles page**

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 (**Figure 34**) is displayed.

OR

Click the **Add A New Value** tab. The Add A New Value tab - Purge Inactive User Profiles page (**Figure 34**) is displayed.

The screenshot shows the 'Purge Inactive User Profiles' page with the 'Add A New Value' tab selected. The page title is 'Purge Inactive User Profiles'. There are two tabs: 'Find an Existing Value' and 'Add a New Value' (active). Below the tabs is a text input field labeled 'Run Control ID:'. Below the input field is an 'Add' button. At the bottom, there are links for 'Find an Existing Value' and 'Add a New Value'.

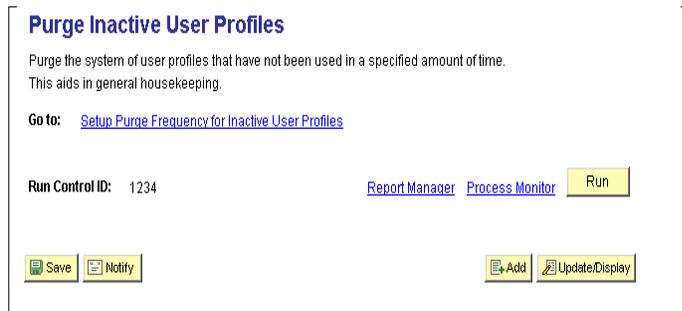
**Figure 34. Add A New Value tab - Purge Inactive User Profiles page**

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 (**Figure 35**) is displayed. For more information, refer to the [User Profiles](#) section of this procedure.



**Figure 35. Purge Inactive User Profiles page**

8. Click the **Setup Purge Frequency For Inactive User Profiles** link. The Password Controls page (**Figure NO TAG**) is displayed. For more information about password controls, refer to the [Password Controls](#) section of this procedure.

## Permissions & Roles

This section contains the following topics:

[Permission Lists](#)

[Copy Permission Lists](#)

[Delete Permission Lists](#)

[Roles](#)

[Copy Roles](#)

[Delete Roles](#)

[Execute Role Rules](#)

### 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 depended upon the organizational needs.

Permission lists include the following:

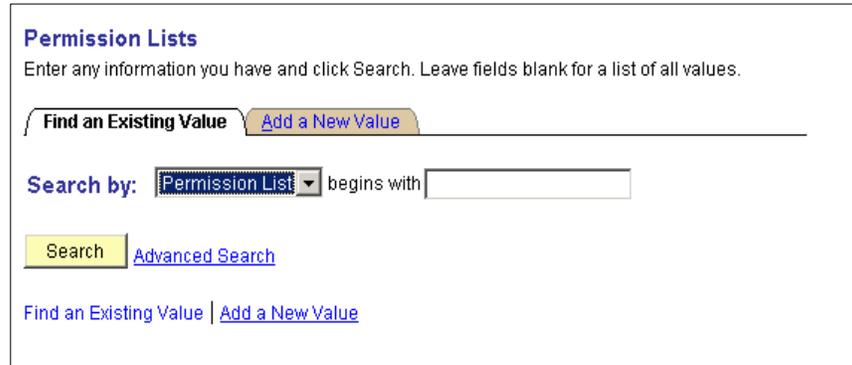
- Singon times
- Page access
- PeopleTools access

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 display either through a Primary list or a Row Security Permission lists.

To add 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 the **Permission Lists**. The Find An Existing Value tab - Permission Lists page **Figure 36)** is displayed.



**Figure 36. Find An Existing Value tab - Permission Lists page**

3. Complete the fields as follows:

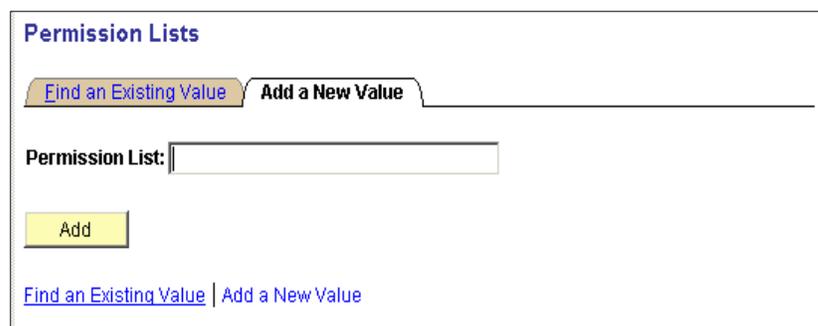
**Search By** This field defaults to **Permission List**. To change, select data from the drop-down list. The valid values are **Permission List** and **Description**.

**Begins With** Enter the information that corresponds to Search By value.

4. Click **Search**. The General tab - Permissions List page (**Figure 38)** is displayed.

**OR**

Select the **Add A New Value** tab. The Add A New Value tab - Permission Lists page (**Figure 37)** is displayed.



**Figure 37. Add A New Value tab - Permission Lists page**

5. Complete the field as follows:

**Permission List**                      Enter the applicable information.

6. Click **Add**. The General tab -Permission List page (**Figure 38**) is displayed. This tab sets general or miscellaneous attributes and system defaults.

**Figure 38. General tab - Permission List page**

7. Complete the fields as follows:

**Permission List**                      This field is 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.

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

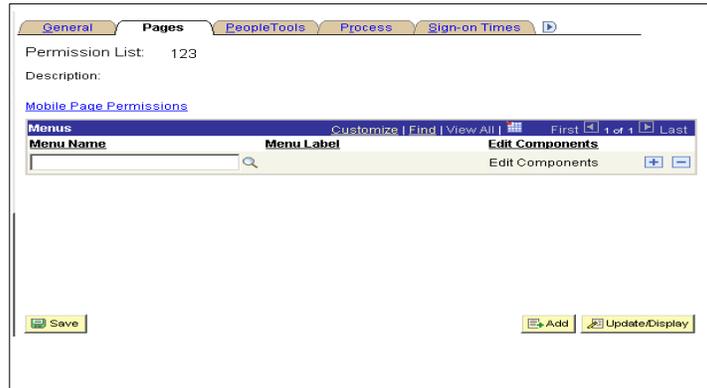
**Can Start Application Server?**                      Check this box if applicable.

**Allow Password To Be Emailed?**                      Check this box if applicable.

**Never Time-out**                              This box is 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 Pages tab-Permission List page (**Figure 39**) is displayed. This tab set page permissions.



**Figure 39. Pages tab - Permission List page**

9. Complete the fields as follows:

**Permission List**

This field is populated based on the search criteria entered.

**Description**

This field is populated based on the description entered on the General tab - Permission List page (**Figure 38**)

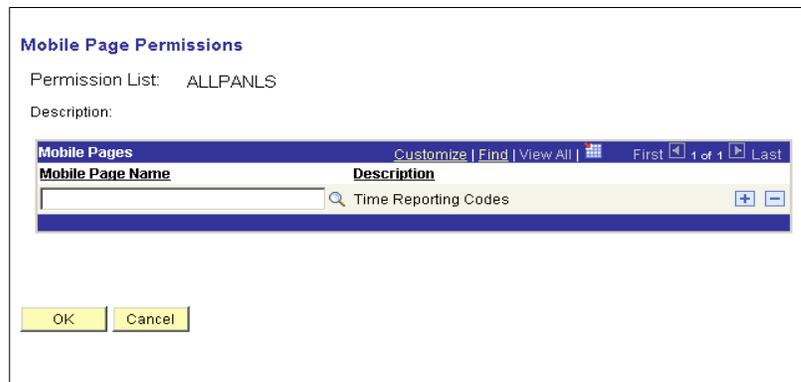
**Menu Name**

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

**Menu Label**

This field is populated based on the menu name entered.

10. Click the **Mobile Page Permissions** link. The Mobile Page Permissions page (**Figure 40**) is displayed.



**Figure 40. Mobile Page Permissions page**

11. Complete the field as follows:

**Permission List** This field is populated based on the search criteria entered.

**Description** This field is populated based on the description entered on the General tab - Permissions page (**Figure 38**).

**Mobile Page Name** Enter the mobile page name or select data by clicking the search icon.

- Click **OK**. The information is saved. The Pages tab - Permission List page (**Figure 39**) is displayed.

OR

Click **Cancel**. The Pages tab - Permission List page (**Figure 39**) is displayed.

- Click the **Edit Components** link. The Component Permissions page (**Figure 41**) is displayed.

Authorized?	Component Name	Item Label	Edit Pages	View Content References for this Component
<input type="checkbox"/>	CBR_PERSONAL_DATA	Modify Personal Information	<a href="#">Edit Pages</a>	<a href="#">View</a>
<input type="checkbox"/>	CBR_PRINT	Reprint Selected Letters	<a href="#">Edit Pages</a>	<a href="#">View</a>
<input type="checkbox"/>	COBRA_ACTIVITY	Review COBRA Triggers	<a href="#">Edit Pages</a>	<a href="#">View</a>
<input type="checkbox"/>	COBRA_DEP_BENEF	Modify Dependent/Beneficiaries	<a href="#">Edit Pages</a>	<a href="#">View</a>
<input type="checkbox"/>	COBRA_EVENT_INQ	Review Event Summary	<a href="#">Edit Pages</a>	<a href="#">View</a>
<input type="checkbox"/>	COBRA_FSA	FSA Benefits	<a href="#">Edit Pages</a>	<a href="#">View</a>
<input type="checkbox"/>	COBRA_HEALTH	Health Benefits	<a href="#">Edit Pages</a>	<a href="#">View</a>
<input type="checkbox"/>	COBRA_MESSAGES	Review Processing Messages	<a href="#">Edit Pages</a>	<a href="#">View</a>
<input type="checkbox"/>	COBRA_PARTIC_ENT1	Participant Elections	<a href="#">Edit Pages</a>	<a href="#">View</a>
<input type="checkbox"/>	COBRA_PARTIC_TERM	Terminate Participant	<a href="#">Edit Pages</a>	<a href="#">View</a>
<input type="checkbox"/>	COBRA_PROG_PARTIC	Assign to Benefit Program	<a href="#">Edit Pages</a>	<a href="#">View</a>
<input type="checkbox"/>	COBRA_RUNCTL	Qualify Event/Proc Enrollment	<a href="#">Edit Pages</a>	<a href="#">View</a>
<input type="checkbox"/>	COBRA_STATUS	Update Event Status	<a href="#">Edit Pages</a>	<a href="#">View</a>
<input type="checkbox"/>	MANUAL_COBRA	Create COBRA Non-Employee	<a href="#">Edit Pages</a>	<a href="#">View</a>
<input type="checkbox"/>	MANUAL_HEALTH	Select Health Benefits	<a href="#">Edit Pages</a>	<a href="#">View</a>
<input type="checkbox"/>	MANUAL_PROG_PARTIC	Assign Benefit Program	<a href="#">Edit Pages</a>	<a href="#">View</a>
<input type="checkbox"/>	RUN_CBR001	Create Initial Letter	<a href="#">Edit Pages</a>	<a href="#">View</a>
<input type="checkbox"/>	RUN_CBR002	Create Secondary Letter	<a href="#">Edit Pages</a>	<a href="#">View</a>
<input type="checkbox"/>	RUN_CBR003	Create Termination Letter	<a href="#">Edit Pages</a>	<a href="#">View</a>
<input type="checkbox"/>	RUN_CBR004	Create Open Enrollment Letter	<a href="#">Edit Pages</a>	<a href="#">View</a>
<input type="checkbox"/>	RUN_CBR005	Event Summary Report	<a href="#">Edit Pages</a>	<a href="#">View</a>
<input type="checkbox"/>	RUN_CBR006	Enrollment Report	<a href="#">Edit Pages</a>	<a href="#">View</a>
<input type="checkbox"/>	RUN_CBR007	Audit Report	<a href="#">Edit Pages</a>	<a href="#">View</a>
<input type="checkbox"/>	RUN_CBR008	Error Report	<a href="#">Edit Pages</a>	<a href="#">View</a>
<input type="checkbox"/>	RUN_CBR009	Create Unavailability Letter	<a href="#">Edit Pages</a>	<a href="#">View</a>

**Figure 41. Component Permissions page**

At this point, the following options are available:

Step	Description
Click <b>Select All</b>	To select all components.
Click <b>Deselect All</b>	To deselect all components.
Click the <b>Edit Pages</b> link.	The Page Permissions page ( <b>Figure 42</b> ) is displayed.



Figure 42. Page Permissions page

14. Complete the field as follows:

**Authorized?** Check this box if applicable.

**Display Only** Check this box if applicable.

**Add** Check this box if applicable.

**Update/Display** Check this box if applicable.

**Update/Display All** Check this box if applicable.

**Correction** Check this box if applicable.

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

**OR**

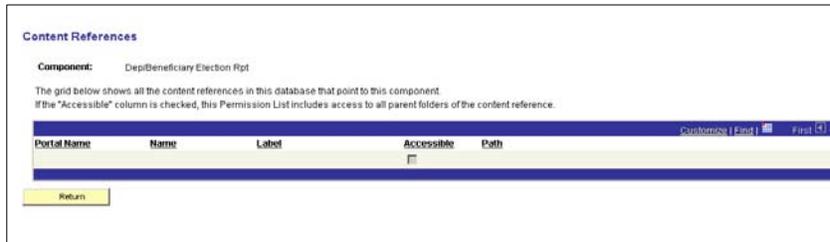
Click **Deselect All** to deselect all components.

16. Click **OK**. The information is saved and the Component Permissions page (**Figure 41**) is displayed.

**OR**

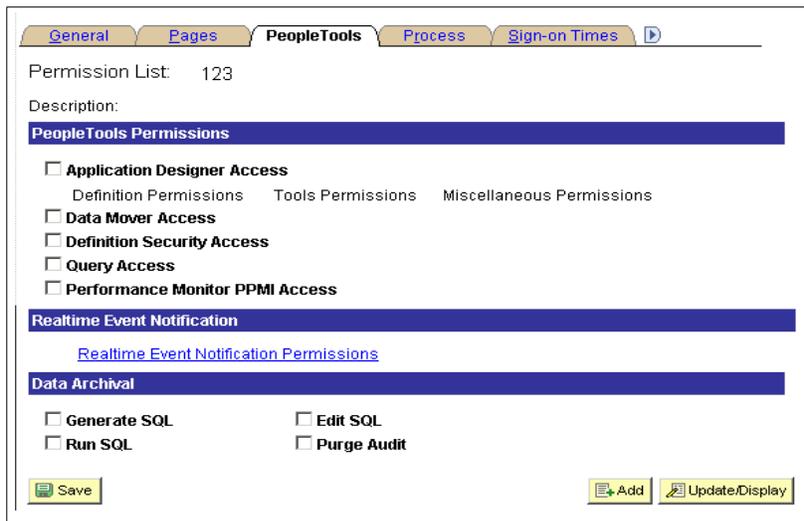
Click **Cancel**. The Component Permissions page (**Figure 41**) is displayed.

17. Click the **Edit** link. The Content References page (**Figure 43**) 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.



**Figure 43. Content References page**

18. Click **Return**. The Component Permissions pages (**Figure 41**) is displayed.
  19. Click **OK** to save the information. The Pages tab - Permission List page (**Figure 39**) is displayed.
- OR**
- Click **Cancel** to cancel the action. The Pages tab - Permission List page (**Figure 39**) is displayed.
20. Select the **People Tools** tab. The Peoples Tools tab - Permission List page (**Figure 44**) is displayed. This tab grants access to the PeopleTools application and grant access for specific options within PeopleTools.



**Figure 44. People Tools tab - Permission List page**

21. Complete the fields as follows:

**Permission List**                      This field is populated based on the search criteria entered.

**Description**                              This field is populated based on the description entered on the General tab - Permission List page (**Figure 38**).

- 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 Move 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 PPMI access.
- 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 (**Figure 45**) is displayed.

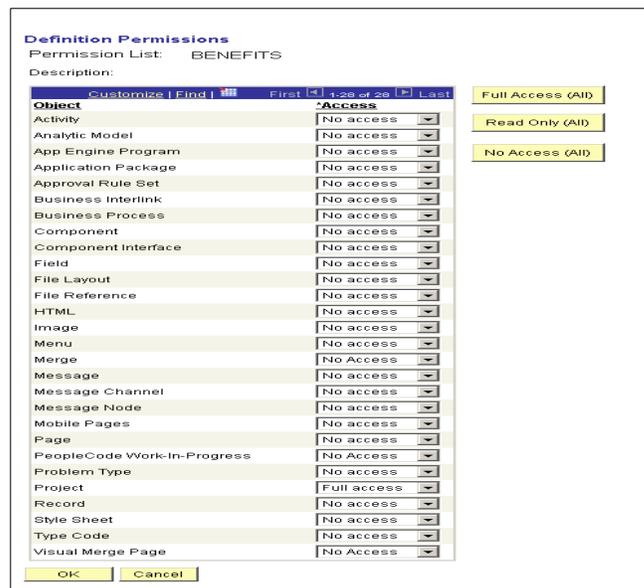


Figure 45. Definition Permissions page

23. Complete the fields as follows:

- |                        |  |
|------------------------|--|
| <b>Permission List</b> | This field is populated based on the search criteria entered.  |
| <b>Description</b>     | This field is populated based on the description entered on the General tab - Permission List page ( <b>Figure 38</b> ). |
| <b>Object</b>          | This field is populated.   |
| <b>*Access</b>         | Select data from the drop-down list. The valid values are <b>Full Access, No Access, and Read Only Access</b> .          |

At this point, the following options are available:

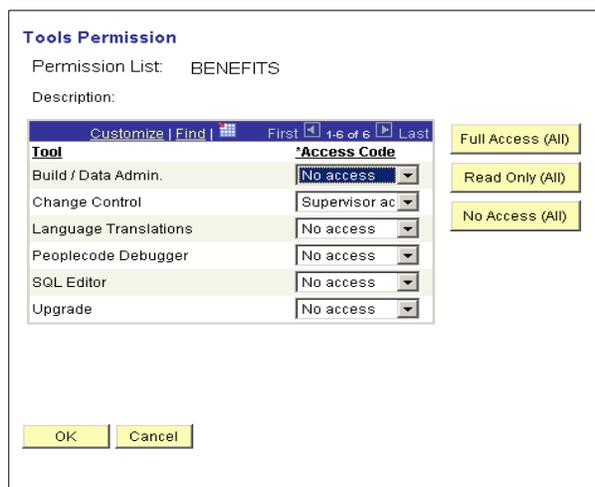
Step	Description
Click <b>Full Access (All)</b>	To apply that value to all objects.
Click <b>Read Only (All)</b>	To apply the read all value to all objects.
Click <b>No Access (All)</b>	To apply the not access value to all objects.

24. Click **OK** to save the data. The People Tools tab - Permission List page (**Figure 44**) is displayed.

**OR**

Click **Cancel** to cancel the action. The People Tools tab - Permission List page (**Figure 44**) is displayed.

25. Click the **Tools Permissions** link. The Tools Permissions page (**Figure 46**) is displayed. The access code drop-down list for each tool listed may vary depending on the permission list selected.



**Figure 46. Tools Permissions page**

26. Complete the fields as follows:

<b>Permission List</b>	This field is populated based on the search criteria entered.
<b>Description</b>	This field is populated based on the description entered on the General tab - Permission List page ( <b>Figure 38</b> ).
<b>Tool</b>	This field is populated.
<b>*Access</b>	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:

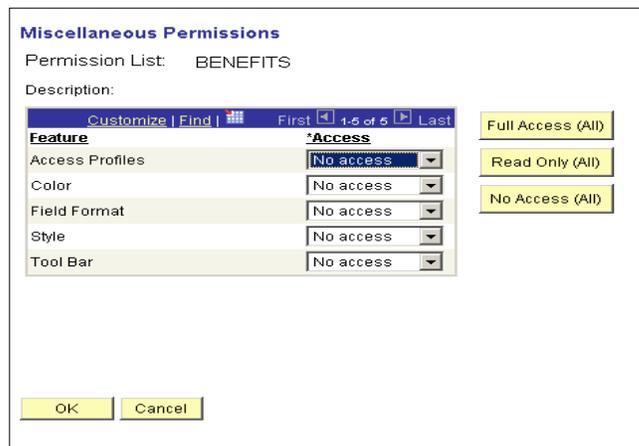
Step	Description
Click <b>Full Access (All)</b>	To apply that value to all objects.
Click <b>Read Only (All)</b>	To apply the read all value to all objects.
Click <b>No Access (All)</b>	To apply the not access value to all objects.

27. Click **OK** to save the data. The People Tools tab - Permission List page (**Figure 44**) is displayed.

**OR**

Click **Cancel** to cancel the action. The People Tools - Permission List page (**Figure 44**) is displayed.

28. Click the **Miscellaneous Permissions** link. The Miscellaneous Permissions page (**Figure 47**) is displayed.



**Figure 47. Miscellaneous Permissions page**

29. Complete the fields as follows:

<b>Permission List</b>	This field is populated based on the search criteria entered.
------------------------	---

<b>Description</b>	This field is populated based on the description entered on the General tab - Permission List page ( <b>Figure 38</b> ).
<b>Feature</b>	This field is populated.
<b>*Access</b>	Enter the applicable information or select data from the drop-down list. The valid values are <b>Full Access</b> , <b>No Access</b> , and <b>Read Only Access</b> .

At this point, the following options are available:

Step	Description
Click <b>Full Access (All)</b>	To apply that value to all objects.
Click <b>Read Only (All)</b>	To apply the read all value to all objects.
Click <b>No Access (All)</b>	To apply the not access value to all objects.

30. Click **OK** to save the data. The People Tools tab - Permission List page (**Figure 44**) is displayed.

**OR**

Click **Cancel** to cancel the action. The People Tools tab - Permission List page (**Figure 44**) is displayed.

31. Click the **Realtime Event Notification Permissions** link. The REN Permissions page (**Figure 48**) is displayed.

**Figure 48. REN Permissions page**

32. Complete the fields as follows:

<b>Permission List</b>	This field is populated based on the search criteria entered.
<b>Description</b>	This field is populated based on the description entered on the General tab - Permission List page ( <b>Figure 38</b> ).

<b>Object</b>	This field is populated.
<b>*Access Code</b>	Enter the applicable information or select data from the drop-down list. The valid values are <b>Full Access</b> , <b>No Access</b> , and <b>Read Only Access</b> .

At this point, the following options are available:

Step	Description
Click <b>Full Access (All)</b>	To apply that value to all objects.
Click <b>Read Only (All)</b>	To apply the read all value to all objects.
Click <b>No Access (All)</b>	To apply the not access value to all objects.

33. Click **OK** to save the data. The People Tools tab - Permission List page (**Figure 44**) is displayed.

**OR**

Click **Cancel** to cancel the action. The People Tools tab - Permission List page (**Figure 44**) is displayed.

34. Select the **Process** tab. The Process tab - Permission List page (**Figure 49**) is displayed. This tab specifies to what capacity a user or role can modify *EmpowHR* Process Scheduler settings.



**Figure 49. Process tab - Permission List page**

35. Complete the fields as follows:

**Permission List** This field is populated based on the search criteria entered.

**Description** This field is populated based on the description entered on the General tab - Permission List page (**Figure 38**).

36. Click the **Process Group Permissions** link. The Process Group Permission page (**Figure 50**) is displayed.



**Figure 50. Process Group Permission page**

37. Complete the fields as follows:

**Permission List**                      This field is populated based on the search criteria entered.

**Description**                              This field is populated based on the description entered on the General tab - Permission List page (**Figure 38**).

**Process Group**                              Enter the process group or select data by clicking the search icon.

38. Click **OK** to save the data. The Process tab - Permission List page (**Figure 49**) is displayed.

**OR**

Click **Cancel** to cancel the action. The Process tab - Permission List page (**Figure 49**) is displayed.

39. Click the **Process Profile Permissions** link. The Process Profile Permission page (**Figure 51**) is displayed.

**Figure 51. Process Profile Permission page**

**40.** Complete the fields as follows:

<b>Permission List</b>	This field is populated based on the search criteria entered.
<b>Description</b>	This field is populated based on the description entered on the General tab - Permission List page ( <b>Figure 38</b> ).
<b>File</b>	Enter the applicable file name for the server destination.
<b>Printer</b>	Enter the applicable printer name for the server destination.
<b>Override Output Destination</b>	Check this box if applicable.
<b>Override Server Parameters</b>	Check this box if applicable.
<b>View Server Status</b>	Check this box if applicable.
<b>Update Server Status</b>	Check this box if applicable.
<b>Enable Recurrence Selection</b>	Check this box if applicable.

- Name** Enter the name for the job controls.
- Acct** Enter the account for the job controls.
- View By** Enter the applicable information or select data from the drop-down list. The valid values are **All**, **None**, and **Owner**.
- Update By** Enter the applicable information or select data from the drop-down list. The valid values are **All**, **None**, and **Owner**.

41. Click **OK** to save the data. The Process tab - Permission List page (**Figure 49**) is displayed.

OR

Click **Cancel** to cancel the action. The Process tab - Permission List page (**Figure 49**) is displayed.

42. Select the **Sign-on Times** tab. The Sign-On-Times tab - Permission List page (**Figure 52**) is displayed. This tab specifies when users are authorized to sign in to the *EmpowHR* application. If users are signed in to the application when the sign-in time expires, they are automatically signed out.

Permission List: 123  
Description:

Day	Start Time	End Time	Time
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	+ -
Sunday	00:00	23:59	+ -

Buttons: Save, Add, Update/Display

**Figure 52. Sign-On Times tab - Permission List page**

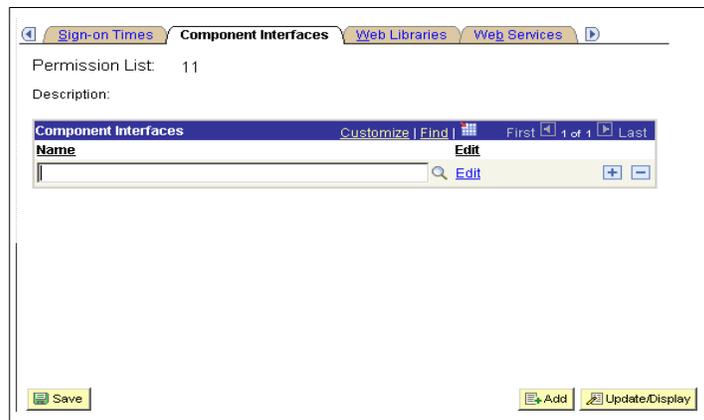
43. Complete the fields as follows:

**Permission List** This field is populated based on the search criteria entered.

**Description** This field is populated based on the description entered on the General tab - Permission List page (**Figure 38**).

- Day** Enter the applicable information or select data from the drop down list. The valid values are **Sunday, Monday, Tuesday, Wednesday, Friday, and Saturday.**
- 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 Component Interfaces tab - Permission List page (**Figure 53**) is displayed. This tab grants access to any component interfaces that a user may need to use to complete a transaction.

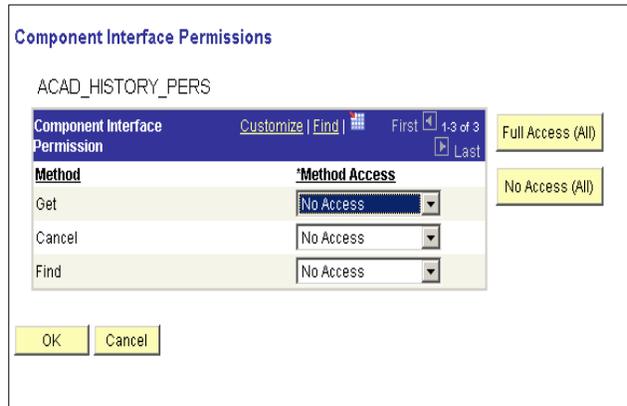


**Figure 53. Component Interfaces tab - Permission List page**

45. Complete the fields as follows:

- Permission List** This field is populated based on the search criteria entered.
- Description** This field is populated based on the description entered on the General tab - Permission List page (**Figure 38**).
- 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 (**Figure 54**) is displayed.



**Figure 54. Component Interface Permissions page**

47. Complete the fields as follows:

<b>Name</b>	This field is populated based on the component interface name entered or selected on the Component Interfaces tab - Permissions page ( <b>Figure 54</b> ) .
<b>Method</b>	This field is populated.
<b>*Method Access</b>	Enter the applicable information or select data from the drop-down list. The valid values are <b>Full Access</b> and <b>No Access</b> .

At this point, the following options are available:

Step	Description
Click <b>Full Access (All)</b>	To apply that value to all objects.
Click <b>No Access (All)</b>	To apply the not access value to all objects.

48. Click **OK** to save the data. The Component Interfaces tab - Permission List page (**Figure 53**) is displayed.

**OR**

Click **Cancel** to cancel the action. The Component Interfaces tab - Permission List page (**Figure 53**) is displayed.

49. Select the **Web Libraries** tab. The Web Libraries tab - Permission List page (**Figure 55**) 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 won't have proper access to the application. If users are not authorized for a particularity web library or script, then cannot invoke it.



Figure 55. Web Libraries tab - Permission List page

50. Complete the fields as follows:

**Permission List**

This field is populated based on the search criteria entered.

**Description**

This field is populated based on the description entered on the General tab - Permissions List page (Figure 38).

**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 (Figure 56) is displayed.

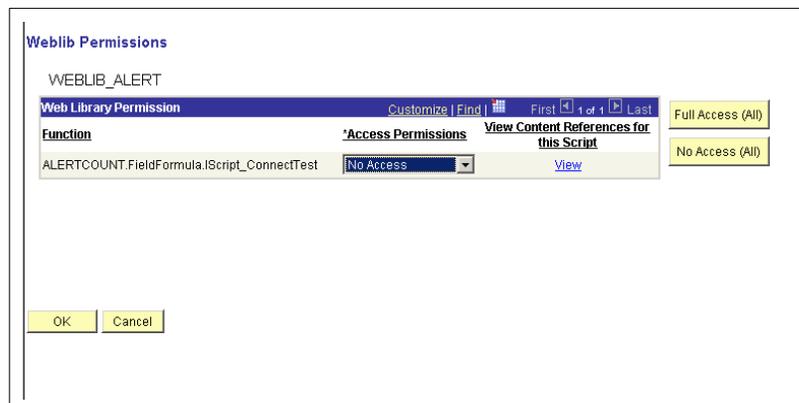


Figure 56. Weblib Permissions page

52. Complete the fields as follows:

**Name**

This field is populated based on the web library name entered or selected on the Web Libraries tab - Permission List page (Figure 55).

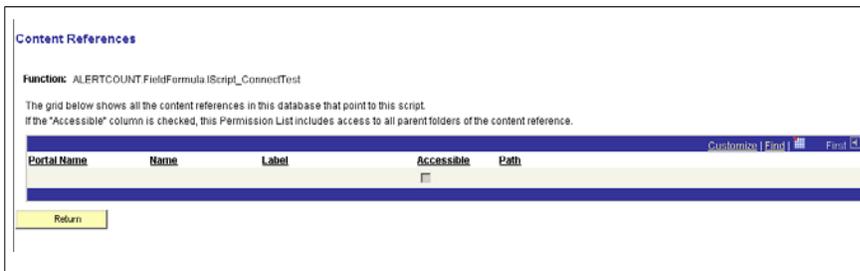
**Function** This field is populated.

**\*Access Permissions** Enter the applicable information or select data from the drop-down list. The valid values are **Full Access** and **No Access**.

At this point, the following options are available:

Step	Description
Click <b>Full Access (All)</b>	To apply that value to all objects.
Click <b>No Access (All)</b>	To apply the not access value to all objects.

- Click the **View** link. The Content References page (**Figure 57**) is displayed. 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.



**Figure 57. Content References page**

- Click **Return**. The Weblib Permissions tab - Permission List page (**Figure 56**) is displayed.
- Click **OK** to save the data. The Weblib Permissions tab - Permission List page (**Figure 55**) is displayed.

**OR**

Click **Cancel** to cancel the action. The Weblib Permissions tab - Permission List page (**Figure 55**) is displayed.

- Select the **Web Services** tab. The Web Services tab - Permission List page (**Figure 58**) is displayed. This page can be customized.

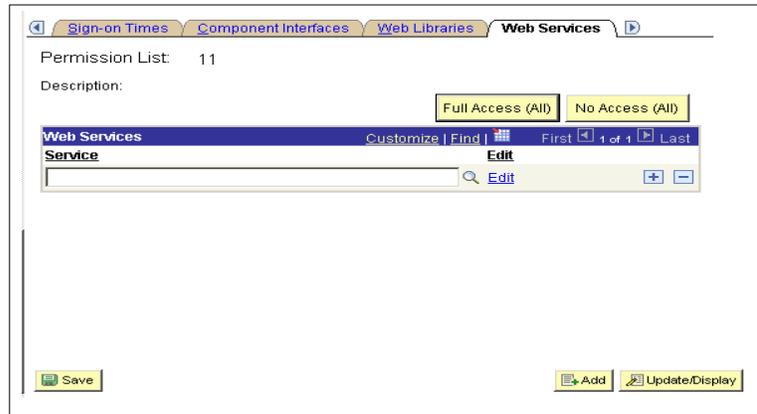


Figure 58. Web Services tab - Permission List page

57. Complete the fields as follows:

**Permission List**

This field is populated based on the value added on the Add A New Value tab.

**Description**

This field is populated based on the Description entered on the General tab - Permission List page (Figure 38). If no data was entered on the General tab (Figure 38), this field will be blank.

**Service**

Enter the applicable service or click the icon to select the applicable service.

58. Click the *Edit* link.

59. Select the **Personalizations** tab. The Personalizations tab - Permission List page (Figure 59) is displayed. This tab sets which personalization users can use and which they can customize.

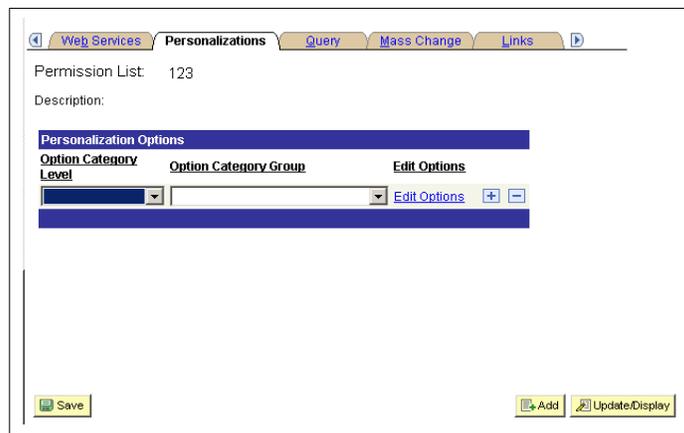


Figure 59. Personalizations tab - Permission List page

60. Complete the fields as follows:

**Permission List** This field is populated based on the search/add criteria entered.

**Description** This field is populated based on the description entered on the General tab - Permission List page (**Figure 38**).

**Option Category Level** Select the applicable data from the drop-down list. The valid values are as follows:

Option Category Level Valid Values
CRM
Custom
EPM
FIN
HRMS
LA
SCM
Tools

**Option Category Group** Select the applicable data from the drop-down list. The valid values are as follows:

Option Category Group Valid Values
App Designer
Preferences
Custom Personalizations
PS Internet Architecture
Portal Personalizations
Query Preferences
Tree Manager Preferences

61. Click the **Edit Options** link. The Personalization Permissions page (**Figure** ) is displayed.

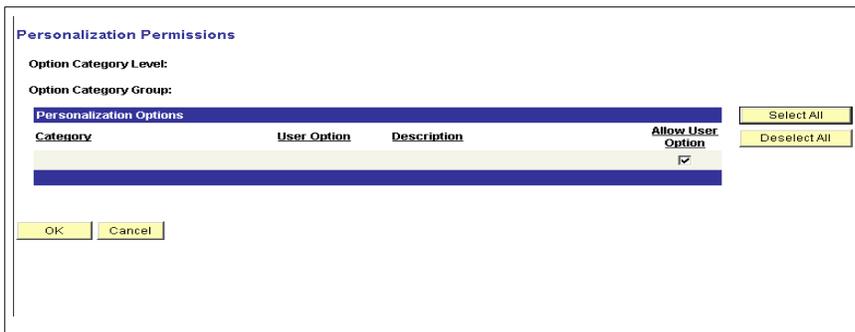


Figure 60. Personalization Permissions page

62. Complete the fields as follows:

<b>Option Category Level</b>	This field is populated from the Personalizations tab - Permission List page.
<b>Option Category Group</b>	This field is populated from the Personalizations tab - Permission List page.
<b>Category</b>	This field is blank and cannot be modified.
<b>User Option</b>	This field is blank and cannot be modified.
<b>Description</b>	This field is blank and cannot be modified.
<b>Allow Users Option</b>	Check this box if the user is allowed to use

At this point, the following options are available:

Step	Description
Click <b>Select All</b>	To select all personalization options.
Click <b>Deselect All</b>	To deselect all personalization options.

63. Click **OK**. The data is saved and the Personalizations tab - Permission List page (**Figure 59**) is displayed.

**OR**

Click **Cancel**. The action is canceled and the Personalizations tab - Permission List page (**Figure 59**) is displayed.

64. Select the **Query** tab. The Query tab - Permission List page (**Figure 61**) is displayed. This tab control the query operations a user can perform and the data they can access while using *EmpowHR* Query.



**Figure 61. Query tab - Permission List page**

65. Complete the fields as follows:

**Permission List** This field is populated based on the search criteria entered.

**Description** This field is populated based on the description entered on the General tab - Permission List page (**Figure 38**).

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

The screenshot shows a dialog box titled "Permission List Access Groups". It contains the following elements:

- Permission List: BENEFITS
- Description:
- A table with the following columns: \*Tree Name, \*Access Group, and Accessible. The Accessible column has a checked checkbox.
- Buttons: OK and Cancel.

Figure 62. Permission List Access Groups page

67. Complete the fields as follows:

**Permission List** This field is populated based on the search/add criteria entered.

**Description** This field is populated based on the description entered on the General tab - Permission List page (**Figure 38**)

**\*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.

68. Click **OK**. The data is saved and the The Permission List Access Groups page (**Figure 62**) is displayed.

**OR**

Click **Cancel**. The action is canceled and the The Permission List Access Groups page (**Figure 62**) is displayed.

69. Select the **Mass Change** tab. The Mass Change tab - Permission List page (**Figure 63**) is displayed. This tab sets mass change security permissions.



**Figure 63. Mass Change tab - Permission List page**

70. Complete the fields as follows:

**Permission List**

This field is populated based on the search/add criteria entered.

**Description**

This field is populated based on the description entered on the General tab - Permission List page (**Figure 38**).

**OK To Execute Online**

Check this box if applicable.

**Mass Change Template ID**

Enter the Mass Change Template ID or select the applicable data by clicking the search icon.

71. Select the **Links** tab. The Links tab - Permission List page (**Figure 64**) is displayed. The links tab is used to view links to other pages within the **EmpowHR** application that pertain to a particular permission list.

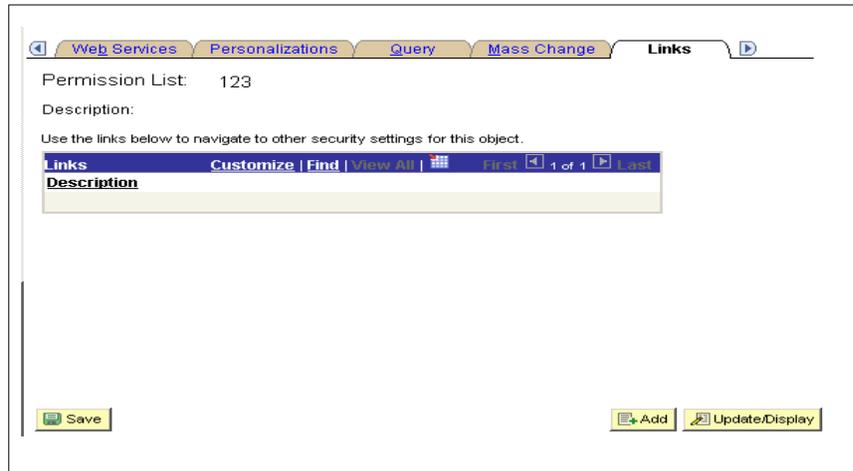


Figure 64. Links tab - Permission List page

72. Complete the fields as follows:

**Permission List** This field is populated based on the search/add criteria entered.

**Description** This field is populated based on the description entered on the General tab - Permission List page (Figure 38).

73. Select the **Audit** tab. The Audit tab - Permission List page (Figure 65) is displayed. This tab allows the user to inquiry when a permission list was last updated and by whom.

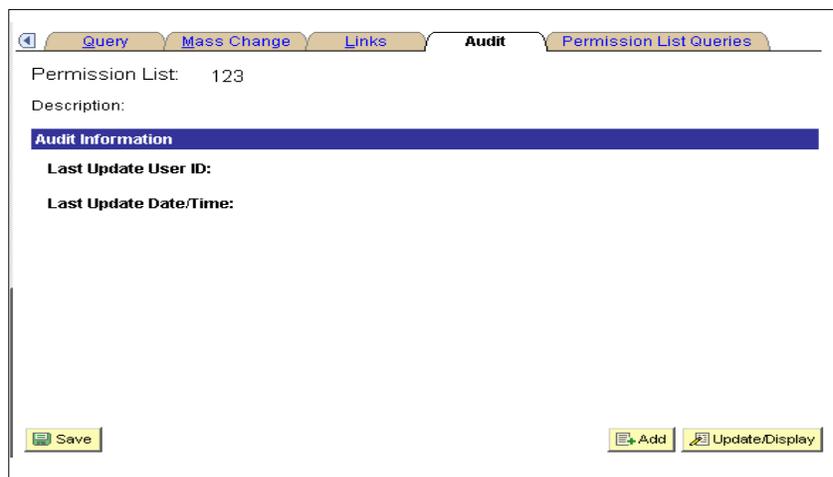


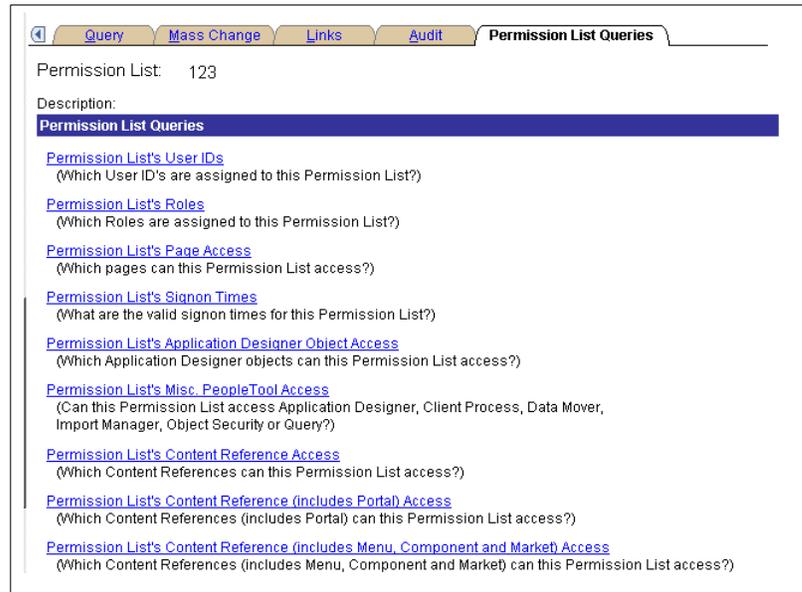
Figure 65. Audit tab - Permission List page

74. Complete the fields as follows:

**Permission List** This field is populated based on the search/add criteria entered.

<b>Description</b>	This field is populated based on the description entered on the General tab - Permission List page ( <b>Figure 38</b> ).
<b>Last Update User ID</b>	This field is populated with the last update.
<b>Last Update Date/Time</b>	This field is populated with the last date/time the User ID was updated.

75. Select the **Permission List Queries** tab. The Permissions List Queries tab - Permission List page (**Figure 66**) is displayed.



**Figure 66. Permission List Queries tab - Permission List page**

76. Complete the fields as follows:

**Permission List** This field is populated based on the search criteria entered.

**Description** This field is populated based on the description entered on the General tab - Permission List page (**Figure 38**).

**Permission List Queries** This field displays a list of links that allow the user to perform queries. Below is a list of the links as follows:

- Click the **Permission List's User IDs** link. This link includes: Which User IDs are assigned to this Permission List?
- Click the **Permission List's Page Access** link. This link includes: Which roles are assigned to this Permission List?

- Click the **Permission List's Signon Times** link. This link includes: What are the valid signon times for this Permission List?
- Click the **Permission List's Application Designer Signon Access** link. This link includes: Which application designer objects can this Permission List Access?
- Click the **Permission List's Page Access** link. This link includes: Which pages can this Permission List access?
- Click the **Permission List's Misc. People Tools Access** link. This link includes: Can this Permission List access application designer, client process, data mover, import manager, object security, or query?
- Click the **Permission List's Content Reference (Includes Portal) Access** link. This link includes: Which content references can this Permission List access?
- Click the **Permission List's Content Reference (Includes Menu, Component, and Market Access** link. This link includes: Which content references (includes Menu, Component, and Market) can this Permission List access?
- Click the **Permission List's Web Service Operation Access** link. This link includes: Which Web Services operation can this Permission List Access?

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

At this point, the following options are available:

Step	Description
Click <b>Add</b>	To return to the Add A New Value tab.
Click <b>Update/Display</b>	To update 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 **Permission Lists** menu item.
4. Select the **Copy Permission Lists** component. The Find An Existing Value tab-Permission List Save As page (**Figure 67**) 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 by:  begins with

[Advanced Search](#)

**Figure 67. Find An Existing Value tab - Permission List Save As page**

- Complete the fields as follows:

<b>Search By</b>	This field defaults to <b>Permission List</b> . To change, select data from the drop-down list. The valid values are <b>Description</b> and <b>Permission List</b> . If <b>Description</b> is selected, the Case Sensitive field is displayed.
<b>Begins With</b>	Enter the information that corresponds to the Search By value selected.
<b>Case Sensitive</b>	Check this box if the criteria is case sensitive. This field is displayed when <b>Description</b> is selected in the Search By field.

- Click **Search**. A list of matches is displayed.
- Select the applicable item on the list. The Permission List Save As page (**Figure 68**) is displayed.

**Permission List Save As**

Save Permission List    ADJUDICATOR To:

**Figure 68. Permission List Save As page**

- Complete the fields as follows:

<b>Save Permission List</b>	This field defaults to the item selected on the list of matches displayed after clicking <b>Search</b> on the Find An Existing Value tab - Permission List Save As page ( <b>Figure 67</b> ).
<b>To</b>	Enter the applicable information.

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

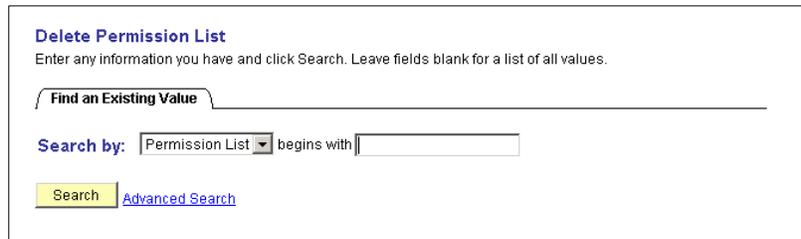
Step	Description
Click <b>Return To Search</b>	To return to the Find An Existing Value tab - Permission List Save As page ( <b>Figure 67</b> ).
Click <b>Refresh</b>	To refresh the page.

### **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 Find An Existing Value tab-Permission List Save As page(**Figure 69**) is displayed.



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

Find an Existing Value

Search by: Permission List begins with

Search Advanced Search

**Figure 69. Find An Existing Value tab - Delete Permission List page**

5. Complete the fields as follows:

<b>Search By</b>	This field defaults to <b>Permission List</b> . To change, select data from the drop-down list. The valid values are <b>Description</b> and <b>Permission List</b> . If <b>Description</b> is selected, the Case Sensitive field is displayed.
<b>Begins With</b>	Enter the information that corresponds to the Search By value selected.
<b>Case Sensitive</b>	Check this box if the criteria is case sensitive. This field is displayed when <b>Description</b> is selected in the Search By field.

6. Click **Search**. A list of matches is displayed.
7. Select the applicable item on the list. The Delete Permission List page (**Figure 70**) is displayed.



**Delete Permission List**

Permission List Id: ADJUDICATOR

Delete Permission List

Return to Search Refresh

**Figure 70. Delete Permission List page**

8. Complete the fields as follows:

**Permission List ID**                      This field is populated based on the item selected on the list of matches.

9. Click **Delete Permission List**. A Delete Permissions Confirmation pop-up (**Figure 71**) appears.



**Figure 71. Delete Permissions Confirmation pop-up**

10. Click **OK** to delete the permission list and return to the Find An Existing Value tab - Delete Permission List page (**Figure 69**).

**OR**

Click **Cancel** to cancel the deletion and return to the Delete Permission List page (**Figure 70**).

## **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 list 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 Roles - Members page is used to display the current list of static role members. the roles-Dynamic Members page 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 the **Permission Lists** menu item.
4. Select the **Roles** component. The Find An Existing Value tab- Roles page (**Figure 72**) is displayed.

**Figure 72. Find An Existing Value tab - Roles page**

5. Complete the fields as follows:

**Search By** Click the down arrow to select the applicable Search By option. This field defaults to **Role Name**. The valid values are **Description** and **Role Name**.

**Begins With** Enter the applicable information.

**Case Sensitive** Check this box if the criteria is case sensitive.

6. Click **Search**. The General tab - Roles page (**Figure 74**) is displayed.

**OR**

Select the **Add A New Value** tab. The Add A New Value tab - Roles page (**Figure 73**) is displayed.

**Figure 73. Add A New Value tab - Roles page**

7. Complete the fields as follows:

**Role Name** Enter the role name.

8. Click **Add**. The General tab - Roles page (**Figure 74**) is displayed.

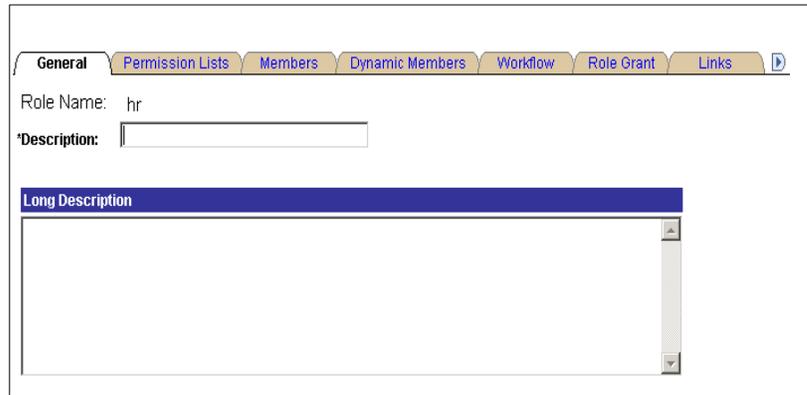


Figure 74. General tab - Roles page

9. Complete the fields as follows:

**Role Name** This field is 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**. The Permission Lists tab - Roles page (Figure 75) is displayed.

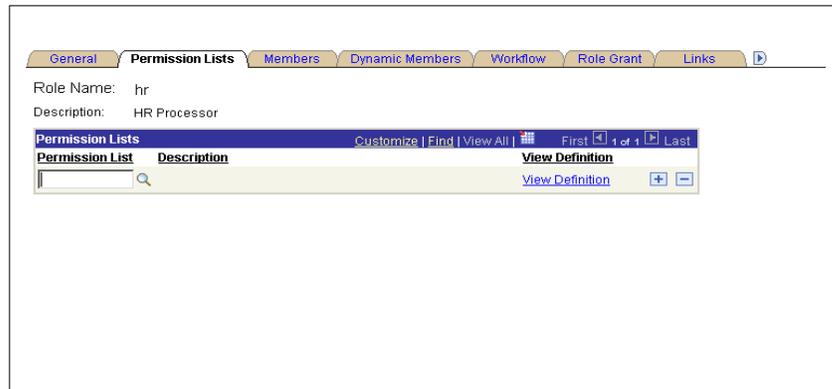


Figure 75. Permission Lists tab - Roles page

11. Complete the fields as follows:

**Role Name** This field is populated with the search/add criteria entered.

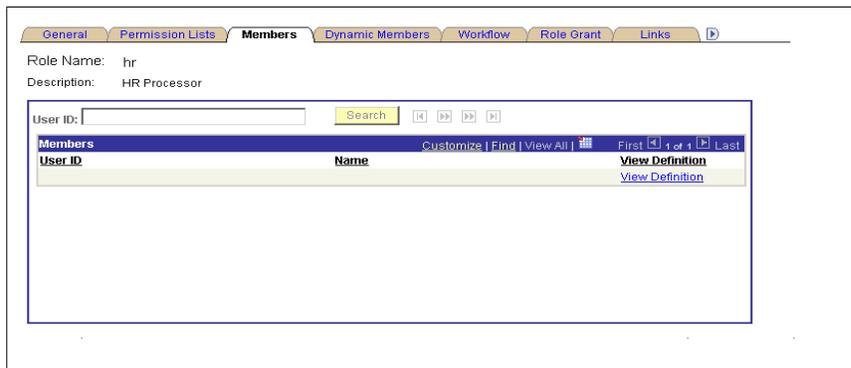
**\*Description** This field is populated with the description of the role name.

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

**Description** This field is used to sort in ascending order.

12. Click the **View Definition** link. The General tab - Permission List page (**Figure 38**) is displayed. For more information about Permission List, refer to the [Permission Lists](#) topic in this procedure.

13. Select the **Members** tab. The Members tab - Roles page (**Figure 76**) is displayed.



**Figure 76. Members tab - Roles page**

14. Complete the fields as follows:

**Role Name** This field is populated with the search/add criteria entered.

**\*Description** This field is populated with the description of the role name.

**User ID** This field is a non-entry field.

**Members/User ID** This field is populated.

**Name** This field is populated.

15. Click the **View Definition** link. The General tab - User Profiles page (**Figure 17**) is displayed. For more information about User Profiles, refer to the [User Profiles](#) topic in this procedure.

16. Select the **Dynamic Members** tab. The Dynamic Members tab - Roles page (**Figure 77**) is displayed.

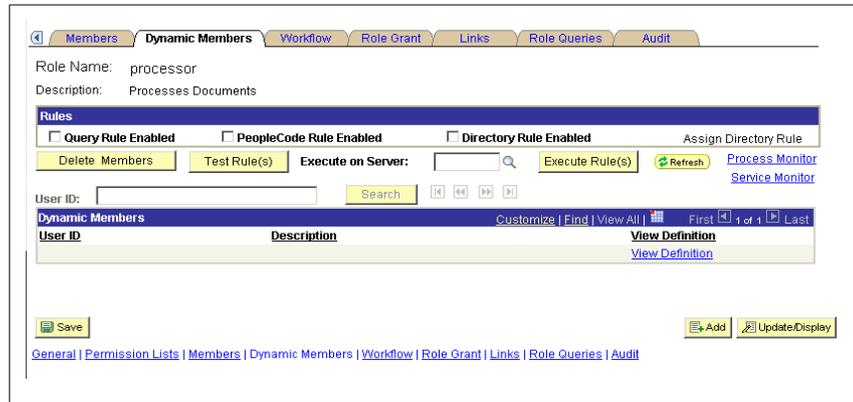


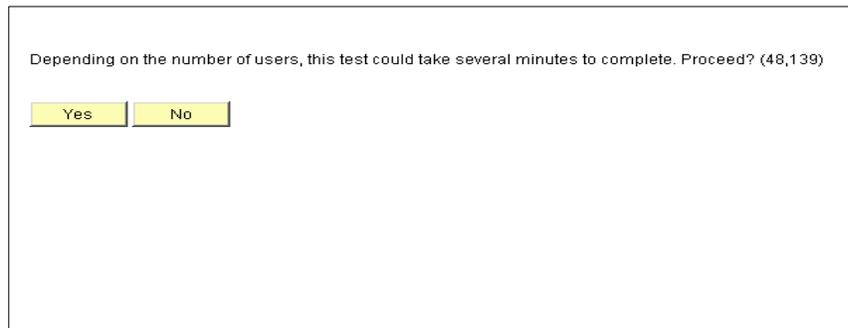
Figure 77. Dynamic Members tab - Roles page

17. Complete the fields as follows:

- |                                 |  |
|---------------------------------|--|
| <b>Role Name</b>                | This field is populated based on the Role Name entered on the General tab - Roles page ( <b>Figure 74</b> ).   |
| <b>Description</b>              | This field is populated based on the Description entered on the General tab - Roles page ( <b>Figure 74</b> ). |
| <b>Query Rule Enabled</b>       | Check this box to enable the query rule.   |
| <b>People Code Rule Enabled</b> | Check this box to enable the people code rule.   |
| <b>Directory Rule Enabled</b>   | Check this box to enable the directory rule.   |
| <b>Execute On Server</b>        | Enter the applicable server name or select a server by clicking the search icon.                               |
| <b>User ID</b>                  | Enter the User ID.   |
| <b>Dynamic Memebers/Uesr ID</b> | This field is populated based on the user ID entered.  |
| <b>Description</b>              | This field is populated based on the user ID entered.  |
| <b>View Definition</b>          | Click this link to view the definition of the dynamic members ID.  |

18. Click **Delete Members** to delete the members listed.

19. Click **Test Rule(s)**. The Test Rules prompt (**Figure 78**) is displayed.

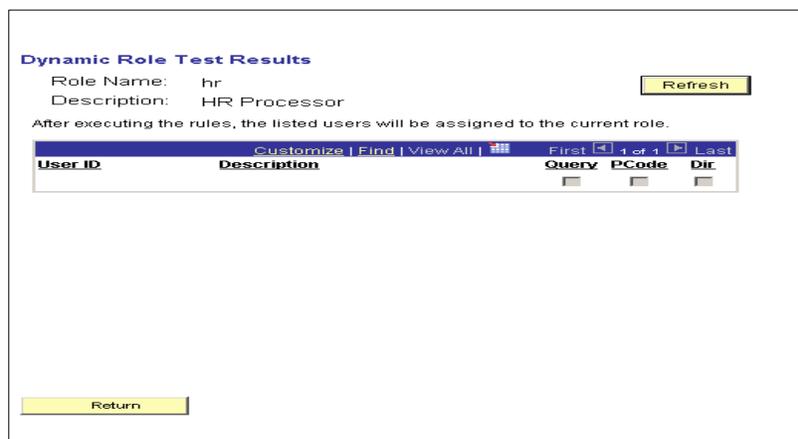


**Figure 78. Test Rules prompt**

20. Click **Yes** to run test rules. The Dynamic Role Test Results page (**Figure 79**) is displayed.

**OR**

Click **No**. The Dynamic Members tab - Roles page (**Figure 77**) is displayed.



**Figure 79. Dynamic Role Test Results page**

21. Click **Execute Rules**. The page is displayed.
22. Click **Refresh** to refresh the page.

**OR**

Click **Process Monitor** to process related reports. For more information, refer to the [Process Monitor](#) topic in this procedure.

**OR**

Click **Service Monitor** if applicable.

23. Select the **Workflow** tab. The Workflow tab - Roles page (**Figure 80**) is displayed. User routing options are set from the Workflow tab - Roles page. 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.

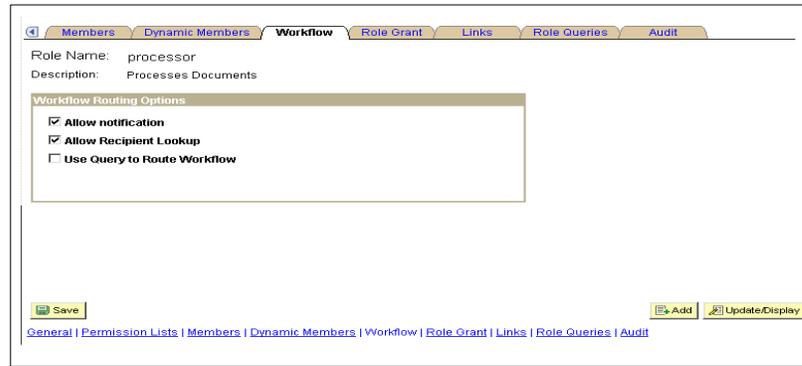


Figure 80. Workflow tab - Roles page

24. Complete the fields as follows:

- |                                    |   |
|------------------------------------|---|
| <b>Role Name</b>                   | This field is populated based on the Role Name entered on the General tab - Roles page ( <b>Figure 74</b> ).  |
| <b>Description</b>                 | This field is populated based on the Description entered on the General tab - Roles page ( <b>Figure 74</b> ).  |
| <b>Allow Notification</b>          | Click this field to allow notification during the workflow process. Users can notify others of data on an <i>EmpowHR</i> page through email or worklist.<br><br>When components are designed, developers can enable the Notify toolbar on the Component Properties dialog box in <i>EmpowHR</i> Application Designer. If this option is set for a particular component, then this checkbox enables security administrators to enable the Notify feature per role. |
| <b>Allow Recipient Lookup</b>      | 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 user in the <i>EmpowHR</i> application. This is available only if the Allow Notification is selected.   |
| <b>Use Query To Route Workflow</b> | 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.  |
| <b>Query Name</b>                  | This field is displayed when you click the Use Query To Route Workflow field. Enter the name of the query to be used when routing workflow or click the icon to search for the applicable query.  |

25. Select the **Role Grant** tab. The Role Grant tab - Roles page (**Figure 81**) is displayed. Users other than security administrators can be given permission to assign roles.

**Figure 81. Role Grant tab - Roles page**

26. Complete the fields as follows:

<b>Role Name</b>	This field is populated based on the Role Name entered on the General tab - Roles page ( <b>Figure 74</b> ).
<b>Description</b>	This field is populated based on the Role Name entered on the General tab - Roles page ( <b>Figure 74</b> ).
<b>Allow Notification</b>	Check this box to allow notification during the workflow process.
<b>Allow Recipient Lookup</b>	Check this box to allow recipient lookup during the workflow process.
<b>Use Query to Route Workflow</b>	Check this box to use query in the workflow process. If this box is checked the query name field is displayed.
<b>Query Name</b>	Enter the name of the query to be used when routing the workflow or select data by clicking the search icon.
<b>Role That Can Be Granted By This Role/Role Name</b>	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 can be granted should report to the granting role.
<b>Role That Can Be Granted By This Role/Description</b>	This field is populated based on the role name selected.

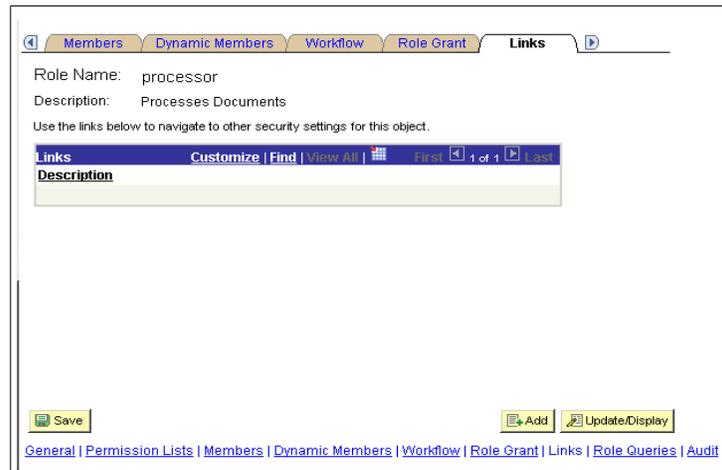
**Roles That Can Grant This Role/Role Name**

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.

**Roles That Can Grant This Role/Description**

This field is populated based on the role name selected.

- 27. Select the **View Definition** link to view the associated definition and make sure that the appropriate definition was selected for the inclusion in the role.
- 28. Select the **Links** tab. The Links tab - Roles page (**Figure 82**) is displayed.



**Figure 82. Links tab - Roles page**

- 29. Complete the fields as follows:

**Role Name**

This field is populated based on the Role Name entered on the General tab - Roles page (**Figure 74**).

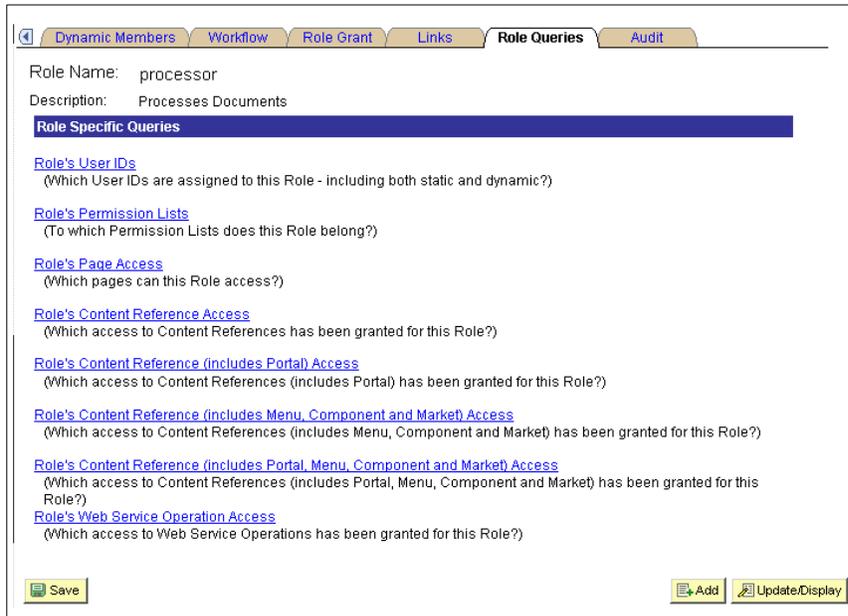
**Description**

This field is populated based on the Role Name entered on the General tab - Roles page (**Figure 74**).

**Description**

Click this field to sort the list by description.

- 30. Click the **Role Queries** tab. The Role Queries tab -Roles page (**Figure 83**) is displayed. This tab includes the following links:



**Figure 83. Role Queries tab - Roles page**

**31. Complete the fields as follows:**

**Role Name** This field is populated based on the Role Name entered on the General tab-Roles page (**Figure 74**).

**Description** This field is populated based on the Role Name entered on the General tab-Roles page (**Figure 74**).

**Role Specific Queries** This field displays a list of links to perform queries. The list of the links are as follows:

**Note:** All available queries are document 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.

At this point, the following options are available:

Link	Description
Click the <b>Role's User ID</b> link.	To view a when a role was last updated and by whom.
Click the <b>Role's Permission Lists</b> link.	Permission list queries enable running queries that provide detailed information regarding a permission such as the User ID and roles associated with a permission list.

Link	Description
Click the <b>Role's Page Access</b> link.	To display a list of pages for which a role as access.
Click the <b>Role's Content Reference Access</b> link.	To display the content associated with certain access.
Click the <b>Role's Content Reference (Includes Menu, Component, And Market)</b> link	To display the (portal) content associated with certain access.
Click the <b>Role's Web Service Operation Access</b> link.	To display Web Service associated with a role.

32. Select the **Audit** tab. The Audit tab - Roles page (**Figure 84**) is displayed. The page is used for auditing purposes.



**Figure 84. Audit tab - Roles page**

33. Complete the fields as follows:

**Role Name** This field is populated based on the Role Name entered on the General tab - Roles page (**Figure 74**).

**Description** This field is populated based on the Role Name entered on the General tab - Roles page (**Figure 74**).

**Last Update User ID** This field is populated.

**Last Update Date/Time** This field is populated.

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

At this point, the following options are available:

Step	Description
Click <b>Add</b>	To return to the Add A New Value tab.
Click <b>Update/Display</b>	To return 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 Find An Existing Value tab- Roles Save As page (**Figure 85**) is displayed.

The screenshot shows a web interface titled "Role Save As". Below the title is a subtitle: "Enter any information you have and click Search. Leave fields blank for a list of all values." There is a tab labeled "Find an Existing Value". Below the tab, there is a "Search by:" section with a dropdown menu currently set to "Role Name" and a text input field labeled "begins with". Below this is a checkbox labeled "Case Sensitive". At the bottom, there is a yellow "Search" button and a blue link for "Advanced Search".

**Figure 85. Find An Existing Value tab - Role Save As page**

5. Complete the fields as follows:

**Search By** This field defaults to **Role Name**. To change, select data from the drop-down list. The valid values are **Description** and **Role Name**.

**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 (**Figure 86**) is displayed.



**Figure 86. Role Save As page**

8. Complete the fields as follows:

**Save Role Name** This field defaults to the item selected on the list of matches displayed after clicking **Search** on the Find An Existing Value Tab - Role Save As page (**Figure 85**).

**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 <b>Return To Search</b>	To return to the Find An Existing Value tab – Permission List Save As page ( <b>Figure 67</b> ).
Click <b>Refresh</b>	To refresh 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 the **Permission Lists** menu item.
4. Select the **Delete Roles** component. The Find An Existing Value tab- Delete Role page (**Figure 87**) 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 by:** Role Name begins with

Case Sensitive

[Advanced Search](#)

**Figure 87. Find An Existing Value tab - Delete Role page**

5. Complete the fields as follows:

**Search By** This field defaults to **Role Name**. To change, select data from the drop-down list. The valid values are **Description** and **Role Name**.

**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 Delete Role page (**Figure 88**) is displayed.

**Delete Role**

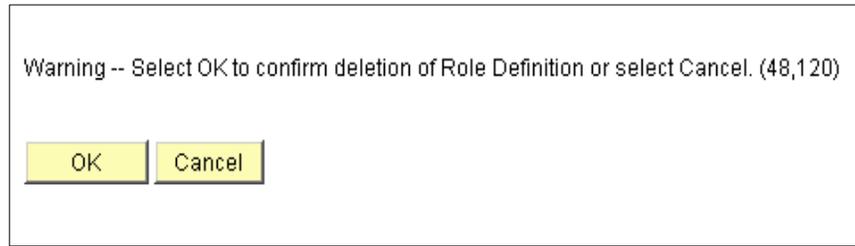
Role Name: ADJUDICATOR

**Figure 88. Delete Role page**

8. Complete the Role Name field as follows:

**Role Name** This field is populated based on the item selected on the Find An Existing Value tab - Role Save As page (**Figure 85**).

9. Click **Delete Role**. A Delete Role Confirmation pop-up (**Figure 89**) appears.



**Figure 89. Delete Role Confirmation pop-up**

10. Click **OK** to delete the permission list and return to the Find An Existing Value tab - Delete Role page (**Figure 87**).

**OR**

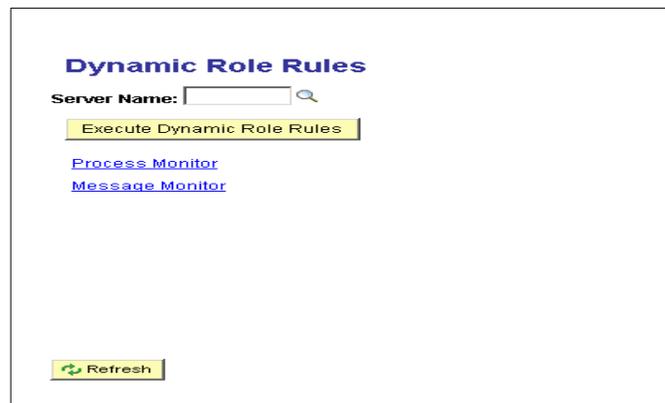
Click **Cancel** to cancel the deletion and return to the Find An Existing Value tab - Delete Role page (**Figure 87**).

### **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 **Permission& Roles** menu item.
4. Select the **Execute Role Rules** component. Dynamic Role Rules page (**Figure 90**) is displayed.



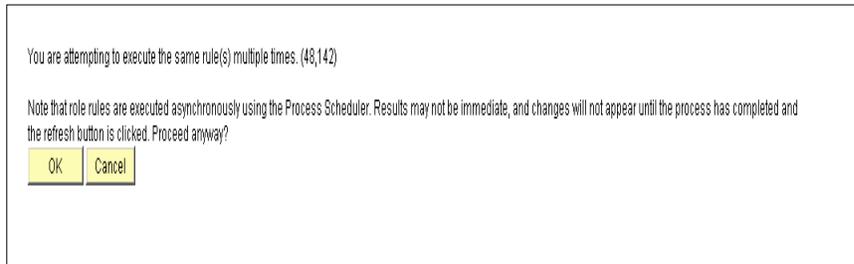
**Figure 90. Dynamic Role Rules page**

5. Complete the Server Name field as follows:

**Server Name**

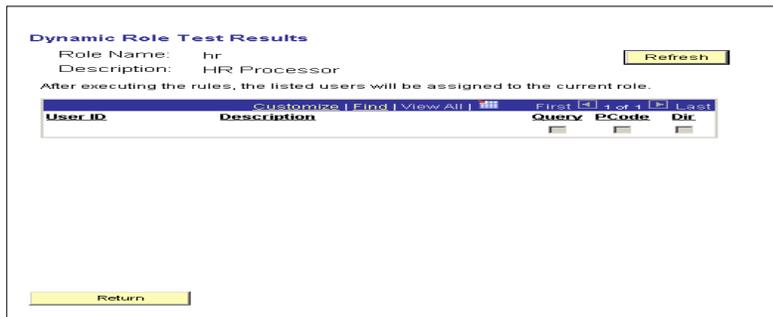
Enter the applicable information or search data by clicking the search icon.

- Click **Execute Dynamic Role Rules**. The Confirmation pop-up (**Figure 91**) is displayed.



**Figure 91. Confirmation pop-up**

- Click **OK**. The Dynamic Role Test Results page (**Figure 92**) is displayed.



**Figure 92. Dynamic Role Test Results page**

- Complete the fields as follows:

<b>Role Name</b>	This field is populated based on the search criteria entered.
<b>Description</b>	This field is populated based on the search criteria entered.

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

<b>User ID</b>	This field is populated with the user IDs assigned to the role name.
<b>Description</b>	This field is populated with the description of the user IDs assigned to the role name.
<b>Query</b>	Check this box if applicable.
<b>PCode</b>	Check this box if applicable.
<b>Dir</b>	Check this box if applicable.

9. Click **Refresh** to refresh the page.
10. Click **Return**. The Dynamic Role Rules page (**Figure 90**) is displayed.

## Password Configuration

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

Password controls help ensure access to the *EmpowHR* applications.

This section contains the following topics:

- [Password Controls](#)
- [Forgotten Password Email Text](#)
- [Forgotten Password Hint](#)
- [Delete Forgotten Password Hint](#)

### Password Controls

The Password Controls page allow 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 Options	Description
Enable Signon Peoplecode	<p>Select this checkbox to enable the following <i>EmpowHR</i> password controls: Age 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>
Age	<p>Use this option to specify the age allowed for passwords.</p> <ul style="list-style-type: none"> <li>• Define a number of days (between 1 and 365) that a password is valid by, selecting the Password Expires in the number of Days option. Users logging on after a password expires must change their password to long on.</li> <li>• Select the Password Never Expires checkbox if you do not want the password to expire.</li> </ul> <p>This option also allows for the specification of the duration that the system wants user when their password is about to expire.</p>

Password Control Options	Description
Account Lock	<p>This control enables locking an account after a <math>x</math> number of failed logon attempts. For instance, if the set Maximum Logon Attempts value to 3, and the user fails three logons, the user is automatically locked out of the application.</p> <p>Setting this control to zero means the account will not be locked out due to erroneous attempts.</p> <p>After the account is locked out, a system security administrator needs to open the user profile and clear the Account Locked checkbox manually.</p>
Miscellaneous	<p>The Allow password to match User ID control enables 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 passwords and User IDs to match.</p>
Minimum Length	<p>Use this control to specify the minimum allowed length for passwords in the application. The value of zero indicates there is no minimum length required, however, the system itself will still require the password to not be blank.</p>
Character Requirements	<p>Use this section to specify the character requirements for you passwords. Administrators can require a set number of digits or special characters within a password.</p> <p>Special characters, or “specials”, refer to symbols such as # and @, and digits refer to number (integers), such as 1 or 2.</p> <p>A List of characters that can be included within a password are: ! @ # \$ % ^ &amp; * &amp; * () _ = + \   ] [ { } ; : / ? . &lt; &gt;</p>
Purge User Profiles	<p>This setting enables purging the system of user profiles that have not been used in a specified amount of time. This aids in general housekeeping. This directive outlines the policy, responsibility, and procedures for the disposal of unused user accounts.</p> <p>As new agencies and employees are implemented into <b>EmpowHR</b>, the number of user accounts and security vulnerabilities increase proportionately. Consequently, in order to maintain control of security files, guidelines for the disposal of unused user accounts must be enforced</p> <p>Notifications of user accounts not used for a period of 30 days and 60 days will be sent to division/staff security coordinators and agency security officers. Any user account not used for a period of 60 days will be suspended or de-activated. Any user account not used for a period of 120 days will be deleted from all platforms. Deleted user accounts can only be re-activated for the individual to whom it was originally assigned. For more information refer to Title VII, Chapter 11, Directive 46, Suspension/Deletion of Unused Accessor Identifiers March 30, 2009.</p>

**To access the Password Control 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 (**Figure 93**) is displayed.

Figure 93. Password Controls

5. Complete the fields as follows:

**Enable Signon PeopleCode**

Check this box to enable the Age and Account Lockout password controls. the Age and Account Lockout options are not editable.

**Password Never Expires**

Select this button if the password should never expire.

OR

**Password Expires In Days**

Select this button if the password will expire and enter the number of days the password will be valid.

**Note:** Passwords should expire after 90 days.

**Warn For Days**

Select this button 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.

**Do Not Warn Of Expiration**

Select this button is there should be no warning of the expiration of the password.

**Maximum Long Attempts**

Enter the number of long on attempts before the user is locked out.

<b>Allow Password To Match User ID</b>	Check this box if the user is allowed to match the user ID to the password.
<b>Minimum Password Length</b>	Enter the minimum number of characters designated for the password length.
<b>Required Number Of Specials</b>	Enter the number of special characters designated for the password.
<b>Required Number Of Digits</b>	Enter the required number of digits designated for the password.
<b>Purge User Profiles After Days</b>	Enter the number of days a password can remain inactive before it is purged for the system.
<b>Number Of Passwords To Retain</b>	Enter the number of passwords to be retained in history.

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

**OR**

Click **Schedule**. The Find An Existing Value tab - Purge Inactive User Profiles page(**Figure** ) is displayed.

**Purge Inactive User Profiles**  
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 by:** Run Control ID begins with

Case Sensitive

**Search** [Advanced Search](#)

[Find an Existing Value](#) | [Add a New Value](#)

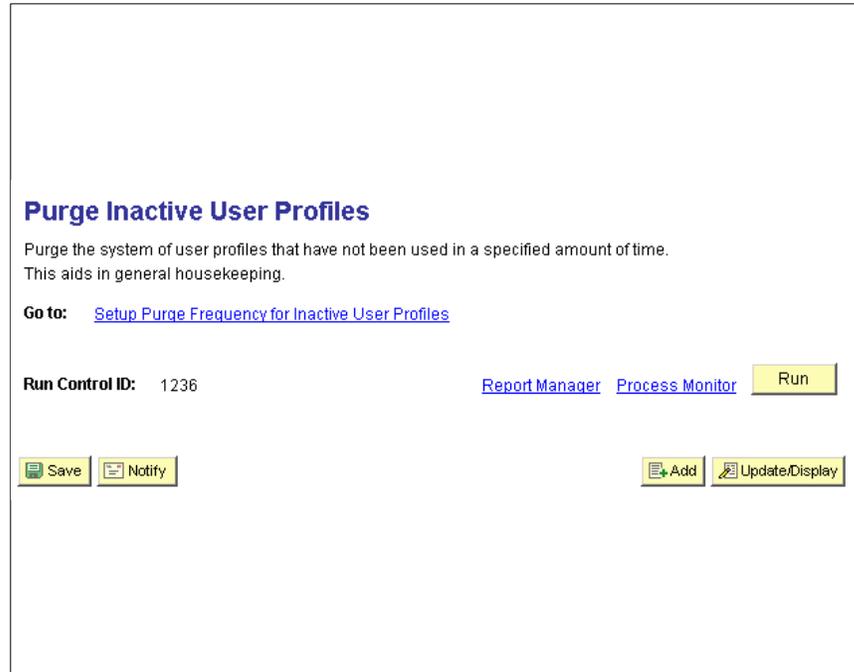
**Figure 94. Find An Existing Value tab - Purge Inactive User Profiles page**

7. Complete the field as follows:

**Search By: Run Control ID Begins With**

Enter the run control ID.

- Click **Search**. The Purge Inactive User Profiles page (**Figure 95**) is displayed.



**Figure 95. Purge Inactive User Profiles page**

- At this point, the following options are available:

Step	Description
Click <b>Save</b>	To save the transaction. The Password Control page( <b>Figure 93</b> ) is displayed.
Click <b>Notify</b>	To notify an email recipient.
Click <b>Add</b>	To return to the Add A New Value tab.
Click <b>Update/Display</b>	To return to the Find An Existing Value tab.
<b>Report Manager</b> link	Refer to Chapter 17, Section 13, Reporting

### **Forgotten Password Email Text**

Before the application email a new, randomly generated password for the forgetful user, make sure they are who they claim to be. 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, then the application automatically email a new password.

When a user has forgotten a password, the application sends the user a new password within an email message. There can 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 just 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 (**Figure 96**) 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: TEST

Save Refresh

**Figure 96. Forgot My Password Email Text**

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.

5. Click **Save**.

**OR**

Click **Refresh** to clear the window.

## Forgotten Password Hint

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

### 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 Find an Existing Value tab - Forgot My Password Hint page(**Figure 97**) is displayed.



**Figure 97. Find An Existing Value tab - Forgot My Password Hint page**

Complete the field as follows:

**Search By: Password Hint ID/Begins With**

Enter the search criteria to find an existing password hint.

5. Click **Search**. The Forgot My Password Hint page (**Figure 99**) is displayed  
OR

Click **Add A New Value** tab to add a new Password Hint. The Add A New Value tab - Forgot My Password Hint page (**Figure 98**) is displayed.

The screenshot shows a web interface titled "Forgot My Password Hint". At the top, there are two tabs: "Find an Existing Value" and "Add a New Value". The "Add a New Value" tab is currently selected. Below the tabs, there is a label "Password Hint ID:" followed by an empty text input field. Underneath the input field is a yellow "Add" button. At the bottom of the form area, there are two blue links: "Find an Existing Value" and "Add a New Value".

Figure 98. Add A New Value tab - Forgot My Password Page

6. Complete the field as follows:

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

7. Click **Add**. The Fort My Password Hint page (**Figure 99**) is displayed.

The screenshot shows the "Forgot My Password Hint" page after the "Add" button was clicked. The page title is "Forgot My Password Hint". Below the title, it says "Password Question ID: 1". There is a label "Active" with a checked checkbox. Below that is a label "Question:" followed by a text input field containing the word "test". At the bottom of the page, there are four buttons: "Save", "Return to Search", "Add", and "Update/Display".

Figure 99. Forgot My Password Hint page

8. Complete the field as follows:

**Active**                                      Verify the Active checkbox is selected.

**\*Question**                                      Enter the verification question.

Step	Description
Click <b>Save</b>	To save the information.
Click <b>Notify</b>	To notify an email recipient.
Click <b>Update/Display</b>	To return to the Find An Existing Value tab.

### **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 Find an Existing Value tab - Delete Forgot My Password Hint page(**Figure** ) is displayed.



**Figure 100. Find And Existing Value tab - Delete Forgot My Password Hint page**

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 (**Figure 101**) is displayed.

**Delete Forgot My Password Hint**

**Password Hint ID:** KAR

**Question:** What is your mother's maiden name

**Last Update Date/Time:** 02/06/09 12:30:27PM

**Last Update User ID:** HFG

**Delete**

**Figure 101. Delete Forgot My Password Hint page**

- Complete the fields as follows:

<b>Password Question ID</b>	This field is populated based on the search criteria entered.
<b>Active</b>	This box is checked when a challenge question is established or added.
<b>*Question</b>	This field is populated based on the search criteria entered. Enter a challenge question when adding a new value.

- Click **Delete** to delete the password hint. The Find A Existing Value tab - Delete Forgot My Password Hint page (**Figure 100**) is displayed.

Step	Description
Click <b>Save</b>	To save the information.
Click <b>Return To Search</b>	To return to Find An Existing Value tab - Delete Forgot My Password Hint page ( <b>Figure 100</b> ).
Click <b>Refresh</b>	To refresh the window.

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

## Security Objects

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

This section contains the following topics:

[User Profile Types](#)

[Tables to Skip](#)

[Security Links](#)

[Digital Signature](#)

[Single Signon](#)

[Signon Peoplecode](#)

## User Profile Types

To update/add a user profile type:

1. Select the **People Tools** menu group.
2. Select the **Security Objects** menu.
3. Select the **User Profile Types** component. The Find An Existing Value tab - User Profile Types page (**Figure 102**) is displayed.

**User Profile Types**  
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 by: ID Type begins with

Search | Advanced Search

Find an Existing Value | Add a New Value

**Figure 102. Find An Existing Value tab - User Profile Types page**

4. Complete the field as follows:

**Search By/ID Type Begins With**                      Enter the ID Type.

5. Click **Search** The User Profile Types page (**Figure 104**) is displayed.

**OR**

6. Click the **Add A New Value** tab. The Add A New Value tab - User Profile Types page (**Figure 103**) is displayed.



- \*Field Name** Enter the name of the user profile.
- \*Record (Table) Name** Enter the table name or select data by clicking the search icon.
- Description Field Name** Enter the description of the field name.

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

### Tables To Skip

Bypass these tables 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 Find An Existing Value tab - Bypass Tables page (**Figure 105**) is displayed. The table(s) listed will be bypassed.

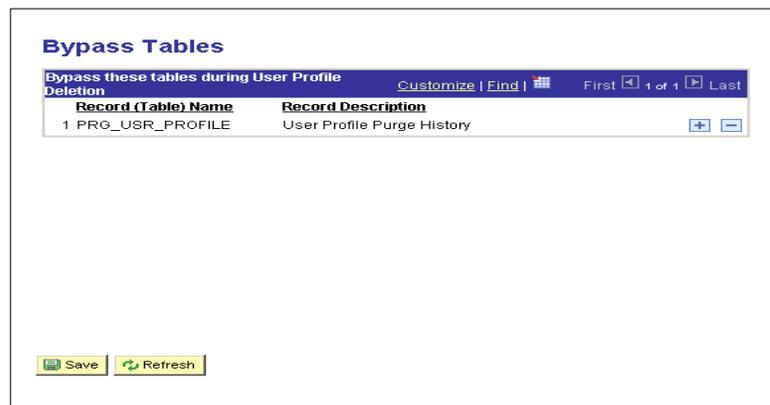


Figure 105. Bypass Tables page

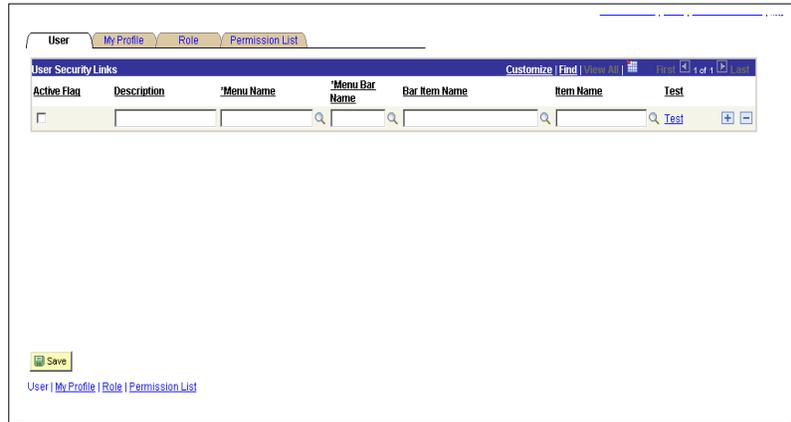
4. Click **Save** to save the information.
5. Click **Refresh** to return to the Find An Existing Value tab - Bypass Tables page (**Figure 105**).

### 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 User tab - Security Links page (**Figure 106**) is displayed.



**Figure 106. User tab - Security Links page**

5. Complete the fields as follows:

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

6. Click the **Test** link. The Find An Existing Value tab - Review AP Extract-Headers page (**Figure 107**) is displayed.

**Review AP Extract-Headers**  
Enter any information you have and click Search. Leave fields blank for a list of all values.

**Find an Existing Value**

SetID:

Vendor ID:

Invoice Number:

Case Sensitive

[Basic Search](#)

**Figure 107. Find An Existing Value - Review AP Extract-Headers page**

7. Complete the fields as follows:

**SetID** Enter the SetID or select data by clicking the search icon.

**Vendor ID** Enter the Vendor ID.

**Invoice Number** Enter the Invoice Number.

**Case Sensitive** Check this box if the search criteria is case sensitive.

8. Click **Search**.

**OR**

Click **Clear** to clear the entries on the page.

9. Select the **My Profile** tab. The My Profile tab - Security Links page (**Figure 108**) is displayed.

User | **My Profile** | Role | Permission List

My Profile User Security Links | Customize | Find |  |  |  |  | 1 of 1 |

Active Flag	Description	Menu Name	Menu Bar Name	Bar Item Name	Item Name	Test
<input type="checkbox"/>		<input type="text" value=""/> <input type="button" value="Q"/>	<input type="text" value="Test"/> <input type="button" value="Q"/>			

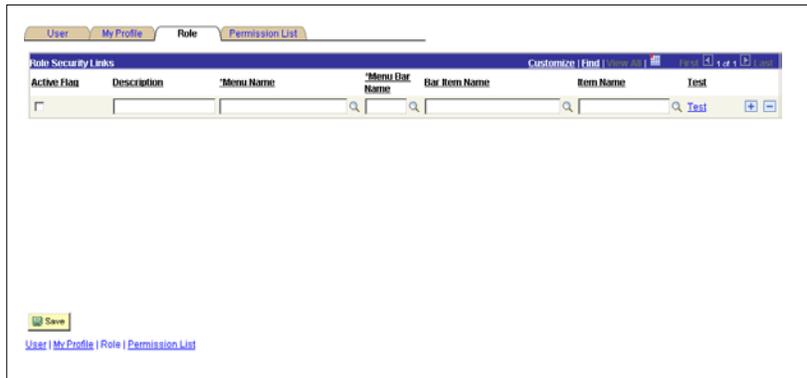
[User](#) | [My Profile](#) | [Role](#) | [Permission List](#)

**Figure 108. My Profile tab - Security Links page**

10. Complete the fields as follows:

- 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.

11. Select the **Role** tab. The My Profile tab - Security Links page (**Figure 109**) is displayed.



**Figure 109. Roles tab - Security Links page**

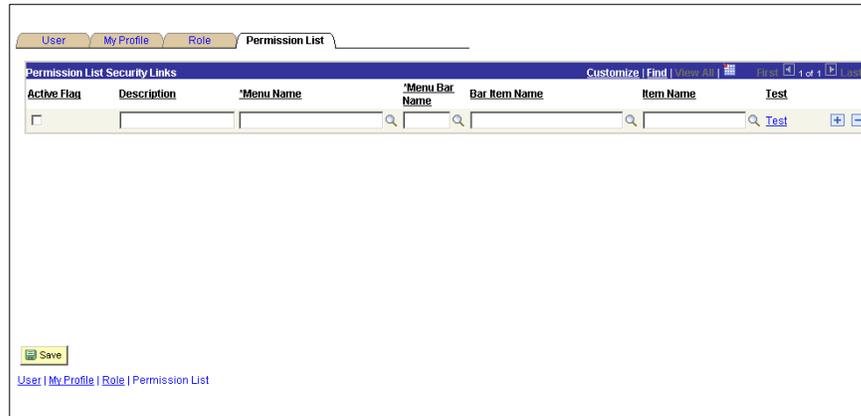
12. Complete the fields as follows:

- 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.

13. Select the **Permission List** tab. The Permission List tab - Security Links page (**Figure 109**) is displayed.



**Figure 110. Permission List tab - Security Links page**

14. Complete the fields as follows:

**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.

15. 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.
4. Select the **Digital Signature** component. The Digital Certificates page (**Figure 111**) is displayed. This page displays the type of certificate, alias and \*issuer alias and valid to (date and time).

Type	Alias	Issuer Alias	Valid to		
Root CA	GTE CyberTrust Global Root	GTE CyberTrust Global Root		<a href="#">Detail</a>	<a href="#">+</a> <a href="#">-</a>
Root CA	GTE CyberTrust Root	GTE CyberTrust Root		<a href="#">Detail</a>	<a href="#">+</a> <a href="#">-</a>
Root CA	KeyWitness Root	KeyWitness Root		<a href="#">Detail</a>	<a href="#">+</a> <a href="#">-</a>
Root CA	PeopleTools TEST root CA	PeopleTools TEST root CA	11/20/23 9:36:28AM	<a href="#">Detail</a>	<a href="#">+</a> <a href="#">-</a>
Root CA	Root SGC Authority	Root SGC Authority	12/31/09 11:00:00PM	<a href="#">Detail</a>	<a href="#">+</a> <a href="#">-</a>
Root CA	Thawte Personal Basic	Thawte Personal Basic	12/31/20 3:59:59PM	<a href="#">Detail</a>	<a href="#">+</a> <a href="#">-</a>
Root CA	Thawte Personal Premium	Thawte Personal Premium	12/31/20 3:59:59PM	<a href="#">Detail</a>	<a href="#">+</a> <a href="#">-</a>
Root CA	Thawte Premium Server	Thawte Premium Server	12/31/20 3:59:59PM	<a href="#">Detail</a>	<a href="#">+</a> <a href="#">-</a>
Root CA	Thawte Server	Thawte Server	12/31/20 3:59:59PM	<a href="#">Detail</a>	<a href="#">+</a> <a href="#">-</a>
Root CA	Verisign Class 1	Verisign Class 1	01/07/20 3:59:59PM	<a href="#">Detail</a>	<a href="#">+</a> <a href="#">-</a>
Root CA	Verisign Class 1 - G2	Verisign Class 1 - G2	05/18/20 4:59:59PM	<a href="#">Detail</a>	<a href="#">+</a> <a href="#">-</a>
Root CA	Verisign Class 2	Verisign Class 2	08/01/28 4:59:59PM	<a href="#">Detail</a>	<a href="#">+</a> <a href="#">-</a>
Root CA	Verisign Class 2 - G2	Verisign Class 2 - G2	05/18/18 4:59:59PM	<a href="#">Detail</a>	<a href="#">+</a> <a href="#">-</a>
Root CA	Verisign Class 3	Verisign Class 3	08/01/28 4:59:59PM	<a href="#">Detail</a>	<a href="#">+</a> <a href="#">-</a>
Root CA	Verisign Class 3 - G3	Verisign Class 3 - G3	05/18/18 4:59:59PM	<a href="#">Detail</a>	<a href="#">+</a> <a href="#">-</a>
Root CA	Verisign Class 3 Public Primary CA	Verisign Class 3 Public Primary CA	08/01/28 4:59:59PM	<a href="#">Detail</a>	<a href="#">+</a> <a href="#">-</a>
Root CA	Verisign Class 4	Verisign Class 4	05/18/18 4:59:59PM	<a href="#">Detail</a>	<a href="#">+</a> <a href="#">-</a>
Root CA	Verisign Class 4 - G4	Verisign Class 4 - G4	08/01/28 4:59:59PM	<a href="#">Detail</a>	<a href="#">+</a> <a href="#">-</a>
Root CA	Verisign/RSA Secure Server CA	Verisign/RSA Secure Server CA	01/07/10 4:59:59PM	<a href="#">Detail</a>	<a href="#">+</a> <a href="#">-</a>

Figure 111. Digital Certificates page

5. Click the **Detail** link. The Certificate Detail -GTE Cyber Trust Global Root page (**Figure 112**) is displayed.

**Certificate Detail - GTE CyberTrust Global Root**

**Subject Information**

**Common Name:** GTE CyberTrust Global Root  
**Org Unit:** GTE CyberTrust Solutions, Inc.  
**Organization:** GTE Corporation  
**Locality:**  
**State/Province:** **Country:** US

**Certificate Information**

**Serial Number:** 421  
**Fingerprint:** CA:3D:D3:68:F1:03:5C:D0:32:FA:B8:2B:59:E8:5A:DB  
**Valid from:** 08/12/1998 20:29:00 **to** 08/13/2018 19:59:00  
**Algorithm:** MD5 with RSA encryption

**Description:**  
 Version: V1  
 Subject: CN=GTE CyberTrust Global Root, OU="GTE CyberTrust Solutions, Inc.", O=GTE Corporation, C=US  
 Signature Algorithm: MD5withRSA, OID = 1.2.840.113549.1.1.4

[Return](#) [Renew](#) [Export](#)

Figure 112. Certificate Detail - GTE Cyber Trust Global Root

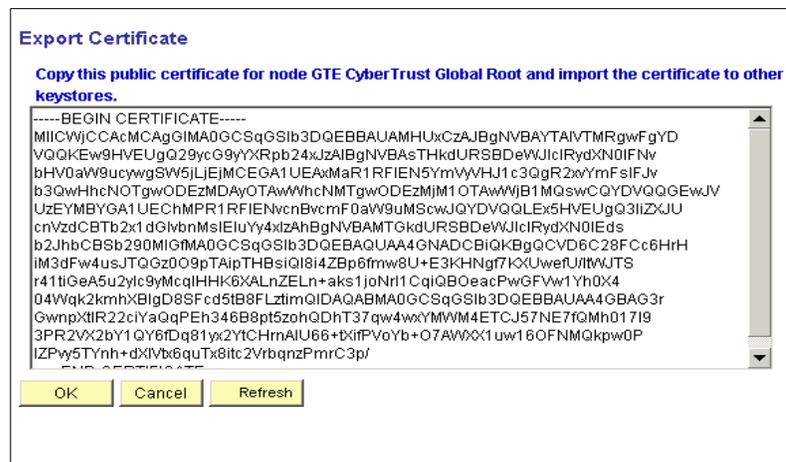
6. Complete the fields as follows:

**Common Name**

This field is populated with the common name for the certificate root.

<b>Org Unit</b>	This field is populated with the organization unit name.
<b>Organization</b>	This field is populated with the organization name.
<b>Locality</b>	This field is populated with the locality if applicable.
<b>State Providence</b>	This field is populated with the state providence if applicable.
<b>Country</b>	This field is populated with the country.
<b>Serial Number</b>	This field is the serial number of the certificate.
<b>Fingerprint</b>	This field is populated with the fingerprint of the person that the certificate relates to.
<b>Valid Dates</b>	This field is the valid dates and the time the certificate was issued.
<b>Algorithm</b>	This field is the methods used issue the certificate.
<b>Description</b>	This field is the description of the algorithm.

7. Click **Review** to review the certificate.
8. Click **Export**. The Export Certificate page (**Figure 113**) is displayed.



**Figure 113. Export Certificate page**

9. Click **OK**.

At this point, the following options are available:

Step	Description
Click <b>Cancel</b>	To return to the Certificate Detail -GTE Cyber Trust Global root page ( <b>Figure 112</b> ).
Click <b>Refresh</b>	To refresh the page.

## Single Signon

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

### To create a Single Signon:

1. Select the **People Tools** menu group.
2. Select the **Security** menu.
3. Select the **Security Objects** menu item.
4. Select the **Single Signon** component. The Single Signon page (**Figure 114**) is displayed.

**Figure 114. Single Signon page**

5. Complete the fields as follows:

**Logon Time In Minutes** This field number of minutes from X to XX,XXX.

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

**Local Node** This field is populated with the local node.

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 (**Figure 115**) is displayed.

*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"/>

**Figure 115. Signon PeopleCode**

**\*Sequence** This field is the populated with the sequence number.

**Enabled** Check this box if the signon is enabled.

**\*Record** This field is record description. To change the record number select data by clicking the search icon.

**\*Field Name** This field is field name. To change the field number select data by clicking the search icon.

**Event** This field is the event default.

**Funtion Name** This field is populated with the function name.

**Exec Auth Fail** Check this box if applicable.

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 to Create query trees to search for existing query trees. How the contents of the query trees are organized depends on the needs of the agency and users.

This section allows the user to define query security.

This section contains the following topics:

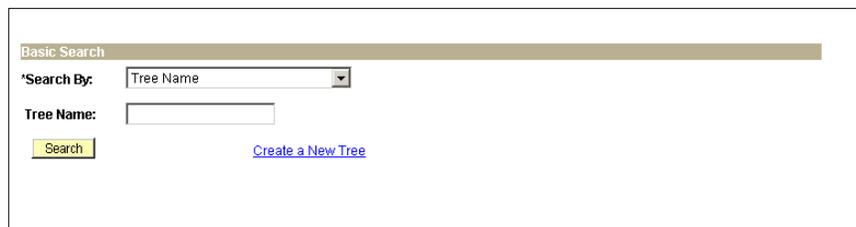
[Query Access Manager](#)

[Query Access List Cache](#)

### 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 Basic Search - Query Access Manager page (**Figure 116**) is displayed.



**Figure 116. Basic Search - Query Access Manager page**

4. Complete the fields as follows:

**\*Search By**

The field defaults to **Tree Name**. To change, select data from the drop-down list. The valid values are as follows:

Search By Valid Values
Tree Name
Group Tree Name Used In A Tree
Record Name Used In A Tree
Tree Category Tree Description

**Tree Name** Enter the tree name.

5. Click **Search**.

OR

Click **Create A New Tree**. The Tree Definition And Properties page (**Figure 117**) is displayed.

The screenshot shows a web form titled "Tree Definition and Properties". The form includes the following fields and options:

- \*Tree Name:** An empty text input field.
- \*Structure ID:** A text input field containing "ACCESS\_GROUP".
- \*Description:** An empty text input field.
- \*Effective Date:** A date input field showing "08/13/2008" with a calendar icon to its right.
- \*Status:** A dropdown menu currently set to "Active".
- \*Category:** A text input field containing "DEFAULT" with a search icon to its right.
- Item Counts:** A box containing "Node Count: 0".
- Tree Change Message Options:** Two radio button options: "Send Tree Change Message" (which is selected) and "Don't send Tree Change Message".
- Buttons:** "OK" and "Return to Search" buttons at the bottom.

**Figure 117. Tree Definition And Properties page**

6. Complete the fields as follows:

**\*Tree Name** Enter the tree name.

**\*Structure ID** This field defaults to **Access-Group** and cannot be changed.

**\*Description** Enter the description of the tree name.

**Effective Date** This field is populated with the current date. To change, select a date from the calendar icon.

**Status** This field defaults to **Active**. To change, select data from the drop-down list. The valid values are **Active** and **Inactive**.

**\*Category** This field defaults to **Default**.

**Node Count** This field defaults to 0.

**Send Tree Change Message** This field is selected. Deselect if applicable.

**Don't Send Tree Change Message** Select this field if applicable

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/nVision. The system can must more quickly 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 the **Query Security** menu.
3. Select the **Query Access List Cache** component. The Query Access List Cache page (**Figure 118**) is displayed.

**Figure 118. Query Access List Cache page**

4. Complete the fields as follows:

**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.

5. Click **Report Manager**. For more information on Report Manager, refer to [Report Manager](#) of this procedure.
6. Click **Process Monitor**. For more information on Process Monitor, refer to [Process Monitor](#) of this procedure.

7. Click **Run**. For more information on Run, refer to [Run](#) of this procedure.

## Common Queries

This section allows the user to maintain 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 (**Figure 119**) is displayed.



**Figure 119. Review Security Information page**

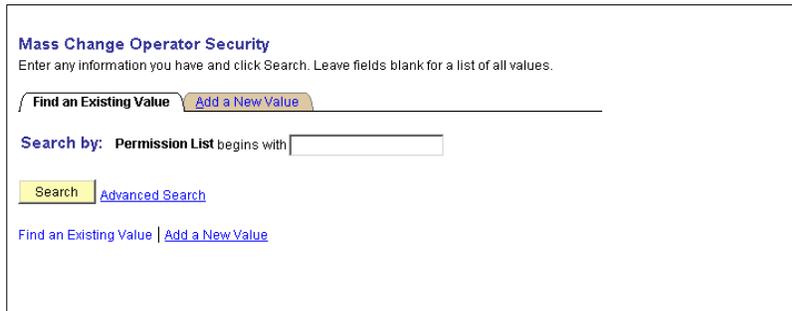
4. Below is a list of links as follows:
  - Click the **Use ID Queries**. This link includes queries specific to a Use ID.
  - Click the **Route Queries** link. This link includes queries specific to a role.
  - Click the **Permission List Queries** link. This link includes queries specific to a permission list.
  - Click the **People Tools Objects Queries** link. This link includes queries specific to a people tolls object.
  - Click the **Definition Security Queries** link. This link includes queries specific to definition security.
  - Click the **Access Log Queries** link. This link includes queries specific 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 Find An Existing Value tab - Mass Change Operator Security page (**Figure 120**) is displayed.



**Figure 120. Find An Existing Value tab - Mass Change Operator Security page**

4. Complete the field as follows:

**Search By Permission List Begins With**      Enter the permission list.

5. Click **Search**. The Security tab page (**Figure 122**) is displayed.

**OR**

Click the **Add A New Value** tab. The Add A New Value tab - Mass Change Operator Security page (**Figure 121**) is displayed.



**Figure 121. Add A New Value tab - Mass Change Operator Security page**

6. Complete the field as follows:

**Permission List**      Enter the permission list.

7. Click **Add**. The Security tab page (**Figure 122**) is displayed.



**Figure 122. Security tab page**

8. Complete the fields as follows:

- |                                |   |
|--------------------------------|---|
| <b>Permission List</b>         | This field is populated based on the search/add criteria entered.             |
| <b>Description</b>             | This field is populated based on the search/add criteria entered.             |
| <b>OK To Execute Online</b>    | Check this box if applicable.   |
| <b>Mass Change Template ID</b> | 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 <b>Notify</b>	To notify the next individual in the workflow.
Click <b>Add</b>	To add an additional mass change operator security.
Click <b>Update Display</b>	To update the page.

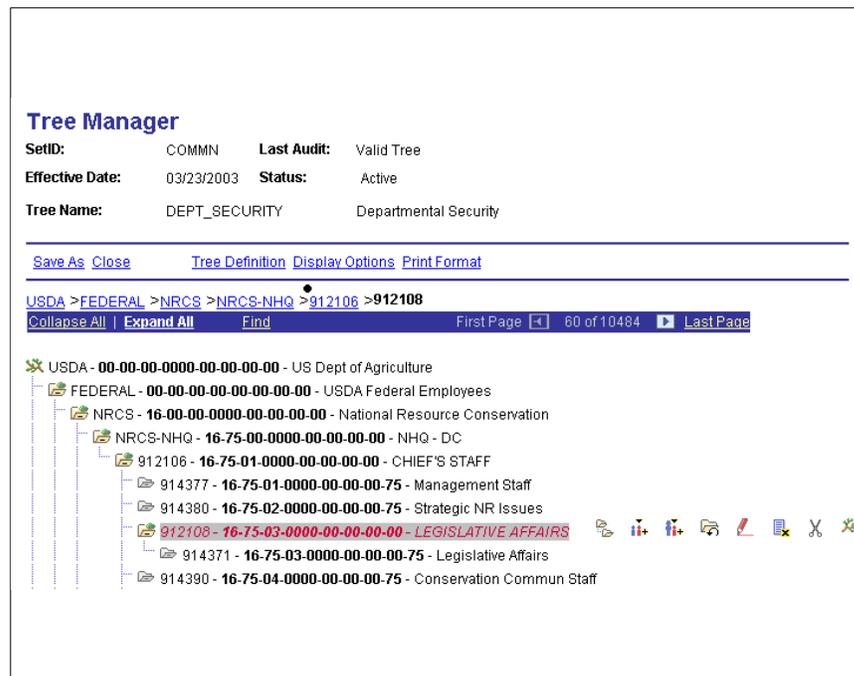


## Tree Manager

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 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 (**Figure 123**).



**Figure 123. Nodes**

Term	Definition
Root Node	The parent folder or the highest level of a hierarchy.
Parent Node	A node that has other nodes reporting to it.
Child Node	A 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 (**Figure 124**) (the horizontal blue bar at the top of the tree).

[Collapse All](#) | [Expand All](#) [Find](#)

Figure 124. Links On Navigation Bar

Action	Description
Collapse	Select to close all of the visible nodes except for the root node. The root node is always expanded.
Expand All	Select to expand all of the nodes on the tree, so that the entire tree or branch hierarchy is visible. Expands all para/child relationships, but the tree hierarchy is still presented one page at a time.
Find	Select to access the Find Value page and search for nodes and detail values.

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

This section contains the following topics:

[Introduction To Tree Manager](#)

[Tree Viewer](#)

[Tree Auditor](#)

[Tree Structure](#)

[Tree Utilities](#)

## Introduction To Tree Manager

To find an existing value on the Tree Manager page:

1. Select **Tree Manager** menu group.
2. Select the **Manager Tree** component. The Find An Existing Value tab - Tree Manager page (**Figure 125**) 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 by:  begins with

Search
[Advanced Search](#)

[Find an Existing Tree](#) | [Create New Tree](#)

Figure 125. Find An Existing Tree tab - Tree Manager page

3. Complete the fields as follows:

**Search By**

This field defaults to **Tree Name**. To change, select data from the drop-down list. The valid values are as follows:

Search By Valid Values
Category
Description
Detail Field
Effective Date
Node Field
Set Control Value
Set ID
Tree Branch
Tree Name
Tree Structure ID
Valid Tree

**Begins With**

Enter the information that corresponds to the Search By valid values.

4. Click **Search**. The Tree Manager page (**Figure 126**) is displayed. Add a new or delete a row from this page.



**Figure 126. Tree Manager page**

OR

5. Select the **Create New Tree** tab. The Create A New Tree tab - Tree Manager page (**Figure 127**) is displayed.

Figure 127. Create New Tree tab - Tree Manager page

- Complete the field as follows:

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

- Click **Add**. The Tree Definition And Properties page (**Figure 128**) is displayed.

Figure 128. Tree Definition And Properties page

- Complete the fields as follows:

**\*Tree Name** This field is 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** This field defaults to **Active**. To change,select date from the drop-down list. The valid values are **Active**, **Freeze**, and **Inactive**.
- \*Description** Enter the description of the tree.
- \*Category** Enter the category or select data by clicking the search icon.
- \*Use Of Levels** This field defaults to **Strictly Enforced**. To change, select data from the drop-down list. The valid values are **Level Not Used**, **Loosely Enforced**, and **Strictly Enforced**.
- 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.
- Node Count** This field is populated.
- Leaf Count** This field is populated.
- Level Count** This field is populated.
- Branch Count** This field is populated.

9. Click **OK**. The Enter Root Node For Tree page (**Figure 129**) is displayed.

Enter Root Node for Tree

Tree Name: TREE 1

Step 1: Set Up Tree Levels

Level Name	All Values	Description	View Detail	Delete Level
------------	------------	-------------	-------------	--------------

Add Level

Step 2: Define Root Node

\*Root Node:

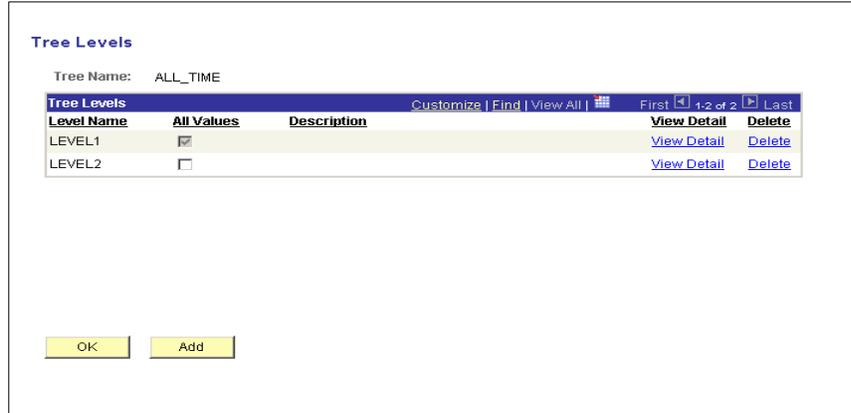
OK Cancel

Figure 129. Enter Root Node For Tree page

10. Complete the fields as follows:

- Tree Name** This field is populated based upon the Tree Name entered on the Create New Tree tab -Tree Manager page (**Figure 127**).
- 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.
- Root Node** Enter the applicable abbreviated Root Node or select data by clicking the search icon.

11. Click **Add Level**. The Tree Levels page (**Figure 130**) is displayed.



**Figure 130. 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** This box checked. Uncheck if applicable.

Click **Save** to save the information.

**OR**

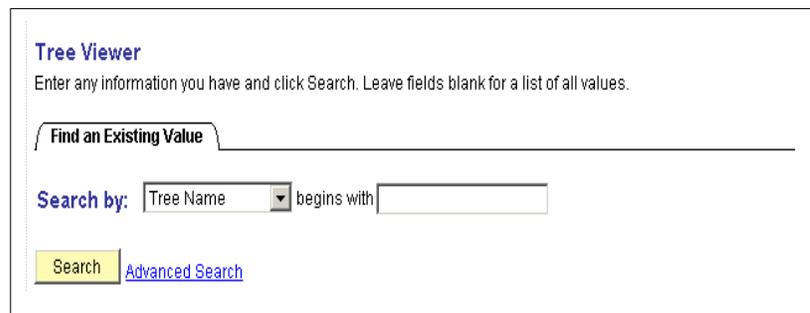
Click **Close** to return to the Enter Root Node For Tree page (**Figure 129**).

## 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 Find An Existing Value tab - Tree Viewer page (**Figure 131**) is displayed.



**Figure 131. Find An Existing Value tab - Tree Viewer page**

3. Complete the fields as follows:

#### Search By

This field defaults to **Tree Name**. To change, select data from the drop-down list. The valid values are as follows:

Search By Valid Values
Category
Description
Detail Field
Effective Date
Node Field
Set Control Value
Set ID
Tree Branch
Tree Name
Tree Structure ID
Valid Tree

#### Begins With

Enter the data that corresponds to the search by field.

4. Click **Search**. The Tree Viewer page (**Figure 132**) is displayed.



Figure 132. Tree Viewer page

5. Complete the fields as follows:

**Set ID** This field is populated from the search criteria entered.

**Last Audit** This field is populated.

**Effective Date** This field is populated with the current date.

**Status** This field is populated with the current status.

**Tree Name** This field is populated with the name of the tree.

**Collaspse All** This link allows the outline of the tree to collapse the folders.

**Expand All** This link allows the outline of the tree to expand the folders.

**Find** This link allows the user to search for a folder.

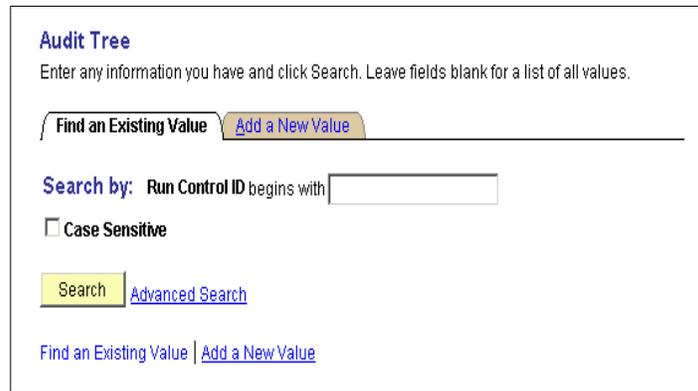
6. Click **Notify** to notify the next individual in the workflow.

## Tree Auditor

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

### To find/add a Tree Auditory:

1. Select the **Tree Manager** menu group.
2. Select the **Tree Auditor** component. The Find An Existing Value tab - Tree Auditor page (**Figure 133**) is displayed.



The screenshot shows the 'Audit Tree' interface. At the top, it says 'Audit Tree' and 'Enter any information you have and click Search. Leave fields blank for a list of all values.' Below this are two tabs: 'Find an Existing Value' (selected) and 'Add a New Value'. A search bar contains the text 'Search by: Run Control ID begins with' followed by an empty input field. Below the search bar is a checkbox labeled 'Case Sensitive'. At the bottom left is a yellow 'Search' button, and next to it is a blue link 'Advanced Search'. At the bottom of the page are two blue links: 'Find an Existing Value' and 'Add a New Value'.

**Figure 133. Find An Existing Value tab - Audit Tree page**

3. Complete the fields as follows:

**Search By/Run Control ID Begins With**

Enter the run control ID.

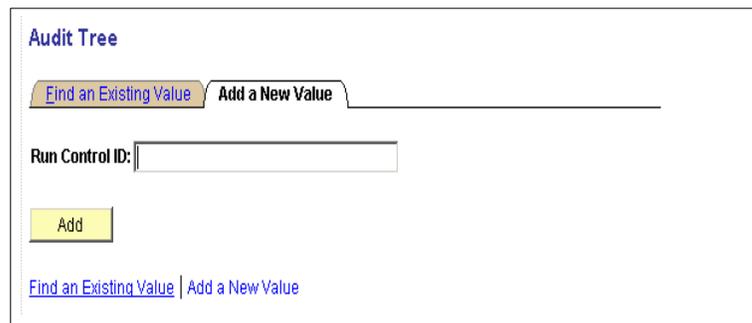
**Case Sensitive**

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

4. Click **Search**. The Tree Auditor page (**Figure 135**) is displayed.

**OR**

Select the **Add A New Value Tab**. The Add A New Value - Audit Tree page (**Figure 134**) is displayed.



The screenshot shows the 'Audit Tree' interface with the 'Add a New Value' tab selected. It features a yellow 'Add' button and a text input field labeled 'Run Control ID:'. At the bottom are two blue links: 'Find an Existing Value' and 'Add a New Value'.

**Figure 134. Add A New Value tab - Audit Tree page**

5. Complete the field as follows:

**Run Control ID**

Enter the run control ID to be added.

- Click **Add**. The Tree Auditor page (**Figure 135**) is displayed.

**Figure 135. Tree Auditor page**

- Complete the fields as follows:

<b>Run Control ID</b>	This field is populated from the search/add criteria entered.
<b>Single Tree</b>	This field is selected. Deselect if applicable.
<b>Multiple Trees</b>	Select this field to select multiple trees.
<b>Tree Name</b>	Enter the tree name or select data by clicking the search icon.
<b>Set ID</b>	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.
<b>Effective Date Of Tree</b>	This field defaults to the current date. To change, select a date from the calendar icon.
<b>As Of Current Date</b>	Enter the as of current date or select a date from the calendar icon
<b>As Of Specific Date</b>	Enter the as of specific date or select a date from the calendar icon
<b>All Trees</b>	Select this field for all trees.

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

Step	Description
Click <b>Notify</b>	To notify the next individual.
Click <b>Add</b>	To return to the Add A New Value tab.
Click <b>Update Display</b>	To update 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 Find An Existing Value tab - Tree Structure page (**Figure 136**) is displayed.

The screenshot shows the 'Tree Structure' page with the following elements:

- Tree Structure** header
- Instruction: "Enter any information you have and click Search. Leave fields blank for a list of all values."
- Two tabs: "Find an Existing Tree Structure" (active) and "Create New Tree Structure"
- Search by:** A dropdown menu currently set to "Tree Structure ID" followed by "begins with" and an empty text input field.
- Buttons: "Search" and "Advanced Search"
- Footer links: "Find an Existing Tree Structure" and "Create New Tree Structure"

**Figure 136. Find An Existing Value tab - Tree Structure page**

3. Complete the fields as follows:

**Search By** This field defaults to **Tree Structure ID**. To change, select data from the drop-down list. The 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 (**Figure 137**) is displayed. This page displays a list of Tree Structure IDs, the Description of the tree ID, and the Tee Structure Type.

Tree Structure ID	Description	Tree Structure Type
<a href="#">TC_DEPT</a>	Dept Tree for Total Comp	Detail
<a href="#">TEST_ADMIN</a>	nI_testadministratie	Detail
<a href="#">TREE_NODE_DISTRIB</a>	Sample Node Distribution	Detail

Figure 137. Search Results page

OR

- Select the **Create A New Tree Structure** tab. The Create A New Tree Structure tab - Tree Structure page (Figure 138) is displayed.

Tree Structure

[Find an Existing Tree Structure](#) **Create New Tree Structure**

Tree Structure ID:

[Find an Existing Tree Structure](#) | [Create New Tree Structure](#)

Figure 138. Create New Tree Structure tab - Tree Structure page

- Complete the fields as follows:

**Tree Structure ID**                      Enter the applicable Tree Structure ID.

- Click **Add**. The Tree Structure Properties tab - Tree Structure page (Figure 139) is displayed.

Structure   [Levels](#)   [Nodes](#)   [Details](#)

**Tree Structure Properties**

Structure ID: TEST

\*Description:

\*Type:

**Additional Key Field**

SetId Indirection

Business Unit

User Defined

None

**Navigation Options**

Node Multi-Navigation

Detail Multi-Navigation

[Structure](#) | [Levels](#) | [Nodes](#) | [Details](#)

Figure 139. Tree Structure Propertiestab - Tree Structure page

- Complete the fields on the Tree Structure Properties page (Figure 139) as follows:

**Structure ID**                                      This field is populated based on the Tree Structure ID entered on the search/add criteria entered.

<b>*Description</b>	Enter the description of the Structure ID.
<b>*Type</b>	This field defaults to <b>Detail</b> . To change,select data from the drop-down list. The valid values are <b>Detail</b> and <b>Summary</b> .
<b>SetID Indirection</b>	This field is selected. Deselect if applicable. If this field is selected,do not select Business Unit, User Defined, or None.
<b>Business Unit</b>	Select this field if applicable. If this field is selected,do not select SetID Indirection, User Defined, or None.
<b>User Defined</b>	Select this field if applicable. If this field is selected,do not select SetID Indirection, Business Unit, or None.
<b>None</b>	Select this field if applicable. If this field is selected,do not select SetID Indirection, Business Unit, or User Defined.
<b>Node Multi-Navigation</b>	Select this field if applicable.
<b>Detail Multi-Navigation</b>	Select this field if applicable.

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

Step	Description
Click <b>Notify</b>	To notify the next individual.
Click <b>Add</b>	To return to the Add A New Value tab.
Click <b>Update Display</b>	To update the page.

## Tree Utilities

This section contains the following topics:

- [Copy/Delete Tree](#)
- [Export Tree](#)
- [Import Tree](#)
- [Repair Tree](#)
- [Repair Tree Reports](#)

### **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 tab - Tree Maintenance page (**Figure 140**) is displayed.

The screenshot shows the 'Tree Maintenance' page with a table of tree definitions. The table has columns for Select, Key Type, User Key, Tree Name, Effective Date, and Valid Tree. The data rows are as follows:

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	BNON	DEPT_SECURITY	01/01/1980	Valid Tree
<input type="checkbox"/>	SetId	BNUSA	DEPT_SECURITY	01/01/1980	Valid Tree
<input type="checkbox"/>	SetId	BEL01	DEPT_SECURITY	01/01/1980	Valid Tree
<input type="checkbox"/>	SetId	NLD02	DEPT_SECURITY	01/01/1980	Valid Tree
<input type="checkbox"/>	SetId	NZL01	DEPT_SECURITY	01/01/1980	Valid Tree
<input type="checkbox"/>	SetId	CAN01	DEPT_SECURITY	01/01/1980	Valid Tree
<input type="checkbox"/>	SetId	HKG01	DEPT_SECURITY	01/01/1980	Valid Tree

**Figure 140. Tree Maintenance page (Tree Maintenance tab)**

4. Complete the fields as follows:

- Select** Check this box to select the applicable line.
- Key Type** This field is populated. Click this field to sort by Key Type.
- User Key** This field is populated. Click this field to sort by User Key.
- Tree Name** This field is populated. Click this field to sort by Tree Name.
- Effective Date** This field is populated. Click this field to sort by Effective Date.
- Valid Tree** This field is populated. Click this field to sort by Valid Tree.

5. Select the **Tree Structure Maintenance** tab. The Tree Structure Maintenance tab -Tree Structure Maintenance page (**Figure 141**) 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_WW
<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_WW	
<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	

**Figure 141. Tree Structure Maintenance tab - Structure Maintenance page**

6. Complete the fields as follows:

<b>Select</b>	Check this box to select the applicable line.
<b>Tree Structure ID</b>	This field is populated. Click this field to sort by Tree Structure ID
<b>Description</b>	This field is populated. Click this field to sort by Description.
<b>Node Record Name</b>	This field is populated. Click this field to sort by Node Record Name.
<b>Detail Record Name</b>	This field is populated. Click this field to sort by Detail Record Name.

At this point, the following options are available.

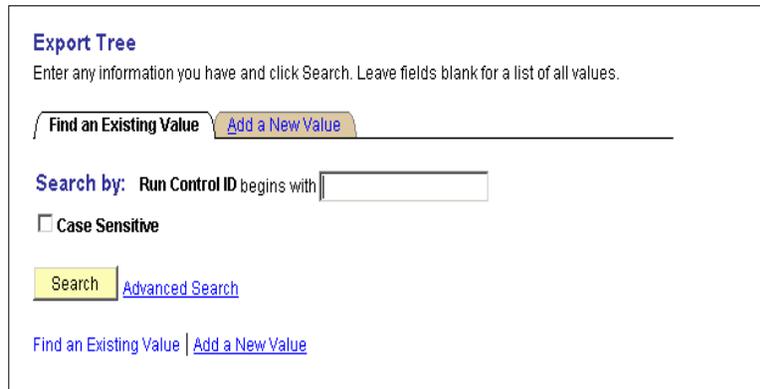
Step	Definition
Click <b>Copy</b>	
Click <b>Delete</b>	
Click <b>View</b>	

### 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 Find An Existing Value tab - Export Tree page (**Figure 142**) is displayed.



**Figure 142. Find An Existing Value tab - Export Tree page**

4. Complete the fields as follows:

**Search By/Run Control ID Begins With**

Enter the Run Control ID.

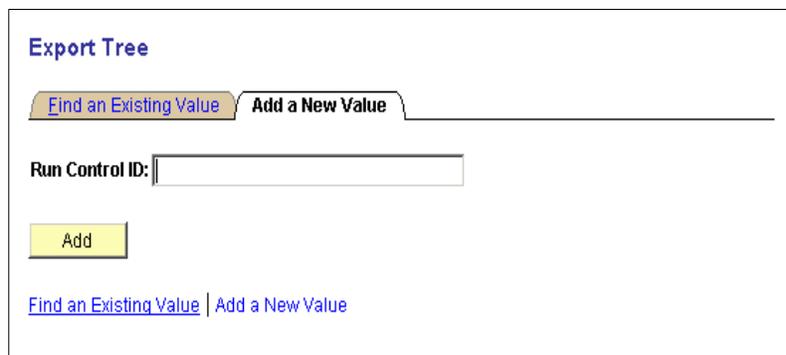
**Case Sensitive**

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

5. Click **Search**. The Tree Export page (**Figure 144**) is displayed.

**OR**

Select the **Add A New Value** tab. The Add A New Value - Export Tree page (**Figure 143**) is displayed.



**Figure 143. Add A New Value tab - Export Tree page**

6. Complete the field as follows:

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

7. Click **Add**. The Tree Export page (**Figure 144**) is displayed.

**Tree Export**

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

\*Output File Name:

**Tree Definition**

Tree Name:   Effective Date:

Tree Key Value:

**Tree Data to Export**

Tree Definition  Tree Structure  Tree User Level  
 Tree Level  Tree Node:Leaf  Tree User Nodes

[Save](#) [Notify](#) [Add](#) [Update/Display](#)

**Figure 144. Tree Export page**

8. Complete the fields as follows:

<b>Run Control ID</b>	This field is populated from the search/add criteria entered.
<b>Output File Name</b>	Enter the output file name.
<b>Tree Name</b>	Enter the tree name or select data by clicking the search icon.
<b>Tree Key Value</b>	Enter the key tree name or select data by clicking the search icon.
<b>Effective Date</b>	Enter the effective date or select a date from the calendar icon.
<b>Tree Definition</b>	This field is populated.
<b>Tree Structure</b>	Check this box to select a tree structure.
<b>Tree User Level</b>	Check this box to select a tree user level.
<b>Tree Level</b>	This field is 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 <b>Notify</b>	To notify the next individual.
Click <b>Add</b>	To return to the Add A New Value tab.
Click <b>Update Display</b>	To update 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 Find An Existing Value tab - Import Tree page (**Figure 145**) 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 by:** Run Control ID begins with

Case Sensitive

[Advanced Search](#)

No matching values were found.

[Find an Existing Value](#) | [Add a New Value](#)

**Figure 145. Find an Existing Value tab - Import Tree page**

4. Complete the fields as follows:

**Search By/Run Control Id BeginsWith** 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 (**Figure 147**) is displayed.

OR

Select the **Add A New Value** tab. The Add A New Value - Import Tree page (**Figure 146**) is displayed.

The screenshot shows a web interface titled "Import Tree". At the top, there are two tabs: "Find an Existing Value" and "Add a New Value", with the latter being the active tab. Below the tabs, there is a text input field labeled "Run Control ID:" containing the text "test". Underneath this field is a yellow button labeled "Add". At the bottom of the form, there are two blue links: "Find an Existing Value" and "Add a New Value".

**Figure 146. Add A New Value tab - Import Tree page**

7. Complete the fields as follows:

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

8. Click **Add**. The Tree Import page (**Figure 147**) is displayed.

The screenshot shows a web interface titled "Tree Import". At the top, there is a "Run Control ID:" field with the value "test" and a yellow "Run" button. Below this are links for "Report Manager" and "Process Monitor". The main section contains several input fields: "Input File Name:" (with a text box), "Save Method:" (with a dropdown menu set to "Save"), and two checked checkboxes: "Replace Tree if Exists" and "Load Tree Defn from File". A section titled "Tree Definition" contains: "Tree Name:" (text box), "Effective Date:" (text box), "Structure:" (text box), "Setid:" (text box), "Description:" (text box), "Category:" (text box with "DEFAULT" selected), and "Use Levels:" (dropdown menu set to "Strictly Enforced"). At the bottom, there are buttons for "Save", "Notify", "Add", and "Update/Display".

**Figure 147. Tree Import page**

9. Complete the fields as follows:

**Run Control ID**                      This field is populated from the search/add criteria entered.

**\*Input File Name**                      Enter the input file name.

**Save Method**                              This field defaults to **save**. To change, select data from the drop-down list. The valid values are **Saved** and **Save Draft**.

**Replace Tree If Exists**                      This box is checked and will replace an existing tree. Uncheck this box if applicable.

<b>Load Tree Defn From File</b>	This box is checked and will load the tree definition from a file. Uncheck this box if applicable.
<b>Tree Name</b>	This field is populated.
<b>Effective Date</b>	This field is populated.
<b>Structure</b>	This field is populated.
<b>All Values</b>	This field is populated.
<b>Allow Duplicate Leaf</b>	This field is populated.
<b>Set ID</b>	This field is populated
<b>Description</b>	This field is populated.
<b>Category</b>	This field is populated.
<b>Use Levels</b>	This field is populated.

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

Step	Description
Click <b>Notify</b>	To notify the next individual.
Click <b>Add</b>	To return to the Add A New Value tab.
Click <b>Update Display</b>	To update 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 Find An Existing Value tab - Repair Tree page (**Figure 148**) is displayed.

**Figure 148. Find An Existing Value tab - Repair Trees page**

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 Tree page (**Figure 150**) is displayed.

OR

Select the **Add A New Value** tab. The Add A New Value - Repair Tree page (**Figure 149**) is displayed.

**Figure 149. Add A New Value tab - Repair Trees page**

6. Complete the fields as follows:

**Run Control ID**

Enter the Run Control ID to be added.

7. Click **Add**. The Repair Tree page (**Figure 150**) is displayed.

Figure 150. Repair Tree page

8. Complete the fields on the Repair Tree page (Figure 150) as follows:

**Run Control ID** This field is populated with the search/add criteria entered.

**\*Tree Utility** This field defaults to **Tree Audits**. To change, select data from the drop-down list. The valid values are as follows:

Tree Utility Valid Values
Tree Audits
Correct Level Numbers
Correct Parent Node Numbers
Delete Orphan Tree Objects
Remove Tree Branches
Remove Tree Reservations
Reset Tree Node Gaps
Update Tree Table Statistics

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

**Set ID** Enter the applicable set ID or select data by clicking the search icon.

<b>Effective Date Of Tree</b>	This field is populated with the current date. To change, select a date from the calendar icon.
<b>As Of Current Date</b>	Select this field if applicable.
<b>As Of Specific Date</b>	This field defaults to the current date. To change, select a date from the calendar icon.
<b>All Trees</b>	Select this field for all trees.

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

Step	Description
Click <b>Notify</b>	To notify the next individual.
Click <b>Add</b>	To return to the Add A New Value tab.
Click <b>Update Display</b>	To update 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 Find An Existing Value tab - Repair Tree Reports page (**Figure 151**) is displayed.

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

Find an Existing Value

Search by: Run Control ID begins with test

Search [Advanced Search](#)

**Figure 151. Find An Existing Value tab - Repair Tree Reports page**

4. Complete the fields as follows:

<b>Search By</b>	This field defaults to <b>Run Control ID</b> . To change, select data from the drop-down list. The valid values are <b>Run Control ID</b> and <b>Process Instance</b> .
------------------	---

**Begins With**

Enter the data that corresponds to the search criteria entered.

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

# Heading Index

This index provides an alphabetical list of all headings in the procedure. When a heading is referenced, you can use this index to locate the page number.

## A

- [Assigning The Distributed Security Administrator Roles To A User, 6](#)
- [Associating Department Security To New Row–Level Permission Lists, 13](#)

## C

- [Common Queries, 103](#)
- [Copy Permission Lists, 60](#)
- [Copy Roles, 74](#)
- [Copy User Profiles, 28](#)
- [Copy/Delete Tree, 119](#)
- [Create And Maintain User Profiles, 18](#)
- [Create New Oprid, 15](#)
- [Creating A Distributed Security Administrator Role, 3](#)
- [Creating A Row–Level Permission List, 11](#)

## D

- [Defining Roles That The Distributed Security Administrator Can Grant, 5](#)
- [Delete Forgotten Password Hint, 87](#)
- [Delete Permission Lists, 61](#)
- [Delete Roles, 75](#)
- [Delete User Profiles, 29](#)
- [Digital Signature, 95](#)
- [Distributed Security Administrator, 8](#)
- [Distributed User Profiles, 31](#)
- [Distributed User Set Up, 32](#)

## E

- [Employee Password Reset, 15](#)
- [EmpowHR User Security \(HD\), 1](#)
- [Execute Role Rules, 77](#)
- [Export Tree, 121](#)

## F

- [Forgotten Password Email Text, 83](#)
- [Forgotten Password Hint, 85](#)

## G

- [Granting Roles And Row–Level Permission Lists, 8](#)

## I

- [Import Tree, 124](#)
- [Introduction To Tree Manager, 108](#)

## M

- [Mass Change Operator Security, 103](#)

## P

- [Password Configuration, 79](#)
- [Password Controls, 79](#)
- [People Tools, 18](#)
- [Permission Lists, 34](#)
- [Permission Lists Overview, 15](#)
- [Permissions & Roles, 34](#)
- [Purge Inactive User Profiles, 33](#)

## Q

[Query Access List Cache, 102](#)

[Query Access Manager, 100](#)

[Query Security, 100](#)

## R

[Repair Tree, 126](#)

[Repair Tree Reports, 129](#)

[Roles, 16](#)

[Roles Component, 63](#)

## S

[Security Objects, 88](#)

[Security Administrator, 3](#)

[Security Links, 91](#)

[Signon Peoplecode, 99](#)

[Single Signon, 98](#)

## T

[Tables To Skip, 91](#)

[Tree Auditor, 114](#)

[Tree Structure, 117](#)

[Tree Utilities, 119](#)

[Tree Viewer, 113](#)

## U

[User Profile Types, 89](#)

[User Profiles, 17](#)

[Profiles \(People Tools\), 18](#)