# Purpose

This document provides guidance for Human Resources (HR) Authorized Requestors (AR) to request changes for their users in the **User Security Request Form** in PeopleSoft. In the form and AR can:

* Assign or delete a user’s security roles for PeopleSoft, Contingent Workforce (a.k.a. FieldGlass) and Harvard Careers
* Clone one user’s access for another user
* Disable a user’s access
* Add or delete a user’s association with:
  + ePerformance Groups
  + Departments
  + Time and Labor Groups (T&L)
  + Absence Groups

# Table of Contents

[Purpose 1](#_Toc57729127)

[Table of Contents 1](#_Toc57729128)

[What to Know Before You Begin 3](#_Toc57729129)

[Security Role Required to Access the Form 3](#_Toc57729130)

[Process Flow for a User Security Request 3](#_Toc57729131)

[How to Get a List of Current Users 4](#_Toc57729132)

[Common Functions Used Throughout the Form 4](#_Toc57729133)

[Lookup/Search 4](#_Toc57729134)

[Navigate Lists 6](#_Toc57729135)

[Create a Request 7](#_Toc57729136)

[Navigate to the User Security Request Form 7](#_Toc57729137)

[Open a User Access Request 8](#_Toc57729138)

[Requisition Information 10](#_Toc57729139)

[Authorized Requestor Information 11](#_Toc57729140)

[User Security Request 11](#_Toc57729141)

[Modify User 12](#_Toc57729142)

[Identify User and Request Details 12](#_Toc57729143)

[Roles 14](#_Toc57729144)

[Current User Roles 14](#_Toc57729145)

[Requested Role Changes 15](#_Toc57729146)

[Delete a Role 15](#_Toc57729147)

[Add a Role 16](#_Toc57729148)

[Group and Department Associations 16](#_Toc57729149)

[Data Permission List 16](#_Toc57729150)

[Current Group and Department Associations 16](#_Toc57729151)

[Requested Group and Department Associations Changes 17](#_Toc57729152)

[Delete an Association 18](#_Toc57729153)

[Add an Association 18](#_Toc57729154)

[Clone User 19](#_Toc57729155)

[Clone Roles, Departments (DPL) and Groups 19](#_Toc57729156)

[Clone DPL Only 22](#_Toc57729157)

[Disable User 22](#_Toc57729158)

[Save and Submit a Request 23](#_Toc57729159)

[Request History 23](#_Toc57729160)

[Find an Existing Request 24](#_Toc57729161)

[25](#_Toc57729162)

[Have Questions? 25](#_Toc57729163)

# What to Know Before You Begin

## Security Role Required to Access the Form

You must have the **“PS^SC^ALL^User Security Form”** role to navigate to and use the **User Security Request Form** in PeopleSoft form. Client Services will grant this role only to HR ARs.

## Process Flow for a User Security Request

1. The HR AR creates and submits a request in the User Security Request Form. For ARs from Central Administration the form name will be User Security Request – CTR.
2. Client Services receives and reviews the request, returns a status change via the form within 48 hours.
3. The HR AR checks the status of the request in PeopleSoft daily:
   1. Approved: Client Services approved request. No further action needed.
   2. Rework: Needs additional work. AR should resubmit the request with the required information described in the Comments field of the Request History section.
   3. Cancelled: Client Services denied the request. See the Comments field of the Request History section for details.
   4. Processed: Client Services processed the request
4. If rework is required, after the AR resubmits the form, the Client Services review process begins again. Returns a status of Processed within 3-5 days.
5. After Client Services processes the request, the AR see the results in Peoplesoft.

Additional statuses may occur during the life of a request and they are all listed in the [Request History and Status](#_Request_History_and) section of this document.

## How to Get a List of Current Users

Log into QlikView, select the University Workforce Application and click on User Security to get a list of your users and the roles currently assigned to them. You must have to the **“HDW^HRO^TUB^No Comp”** role in QlikView to run the User Security List.

## Common Functions Used Throughout the Form

Common functions in the **User Security Request Form** help you navigate through lists and search for users, roles and other items. These elements are used throughout the form but are described once here.

### Lookup/Search

When a magnifying glass is next to a field it indicates you can search for, or lookup, that item. Click on the magnifying glass and a window opens where you can perform the lookup/search. You will see the magnifying glass to lookup an employee, role, group, department, existing request and a few other items within the lookup window itself.

This table describes the fields in a lookup/search window:

| Field Names | Descriptions |
| --- | --- |
| Search Fields | Typically there are a number of fields you can search on and here are a some examples:   * For the User it is:   + Empl Id which is the HUID   + Description which is the employee name * For Role is it the role name * For ePerformance Groups it is the group ID or description.   Enter your search criteria into the text field provided for an ID, Name, etc. |
| Filters | Select an operator for the search criteria you entered in the search field:   * Begins with (when looking up a user’s name, use the last name for begins with) * Contains * = * Not = * < * <= * > * >= * Between * In |
| Look Up Button | Click on it to execute the search based on the search criteria you entered. If the search results have the person, department, etc., that you are looking for, click on it. You will be returned to the main page of the form your selection. |
| Clear Button | Click on it to clear the search criteria so you can enter new criteria. |
| Cancel Button | Click on it to cancel the search and return to the main page of the form. |
| Advance or Basic Search | To the right of the buttons, you will see a link appears that says either Basic or Advance Search. Click on it the link and it will allow you to toggle between Basic and Advance Search. It changes the format of search fields and filters and you may use whichever format you prefer. |
| Case Sensitive checkbox | In the Find an Existing Value search, there is a checkbox you can check to invoke a case sensitive search. |
| Save a search | In the Find an Existing Value search, you can save your search criteria, name it, and use it later. There is also an option to Delete a saved search as well. |

### Navigate Lists

This table describes the navigation elements found at the top right side of lists:

| Field Names | Descriptions |
| --- | --- |
| Find | Click on Find and a small window opens where you can search by a text string. Enter the text and click on the OK button to execute the search. Matching rows are highlighted; if no match is found a message displays to inform you. Click on the Cancel Button to skip the search. |
| View All or View 5 | Click on View All and the list of roles, for example, will expand in the form to show all roles currently assigned to a user. When viewing all roles the function changes to View 5; click on it to go back to listing only the first five roles. |
| New window | Click on the arrow pointing up to the right and a new window will pop open that lists only the roles, for example, currently assigned to the user, all of them. |
| Pagination | Finally, one can navigate a list as follows:   * Click on the left pointing or right pointing arrow to go back and forward in the list, respectively. * Click on the words First or Last to go the beginning or end of the list, respectively.   In between the arrows you can find the number of roles. For example, if it says “1-5 of 55” it means you are looking at the first five roles of 55 roles in total. |

# Create a Request

## Navigate to the User Security Request Form

Log into PeopleSoft and open the Navigation Bar by clicking on the NavBar icon at the top right corner of the window – it is a diamond shape in a circle. The Navigation Bar opens as a column panel on the right side of the window.

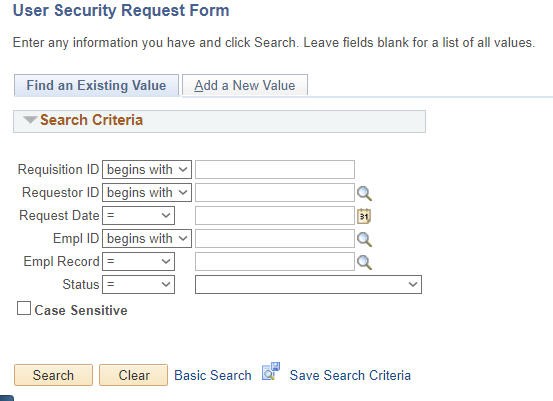
In the Navigation Bar select the icon that is labeled Navigator. A list should display and the you can select Harvard Process, then Entry Forms, and finally the User Security Form. Note, if you were in another section in the Navigation Bar, the name of that section is at the top of the panel; to the left of the section name is an arrow pointing left, select it and you will be returned to the full list of items from where you can select Harvard Processes, then Entry Forms, and finally the User Security Form.

A window opens where you may opt to find an existing request or start a new request.

Note, the terms request and requisition are used interchangeably.

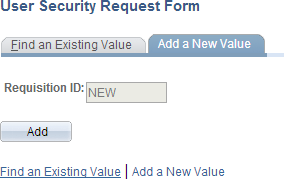
## Open a User Access Request

After navigating to the form as described in the [navigation section](#_Navigate_to_the), you will come to a window with two tabs. In the first tab you can **Find an Existing Value**, a.k.a. an existing request, and in the second you can **Add a New Value**, a.k.a. a new request.

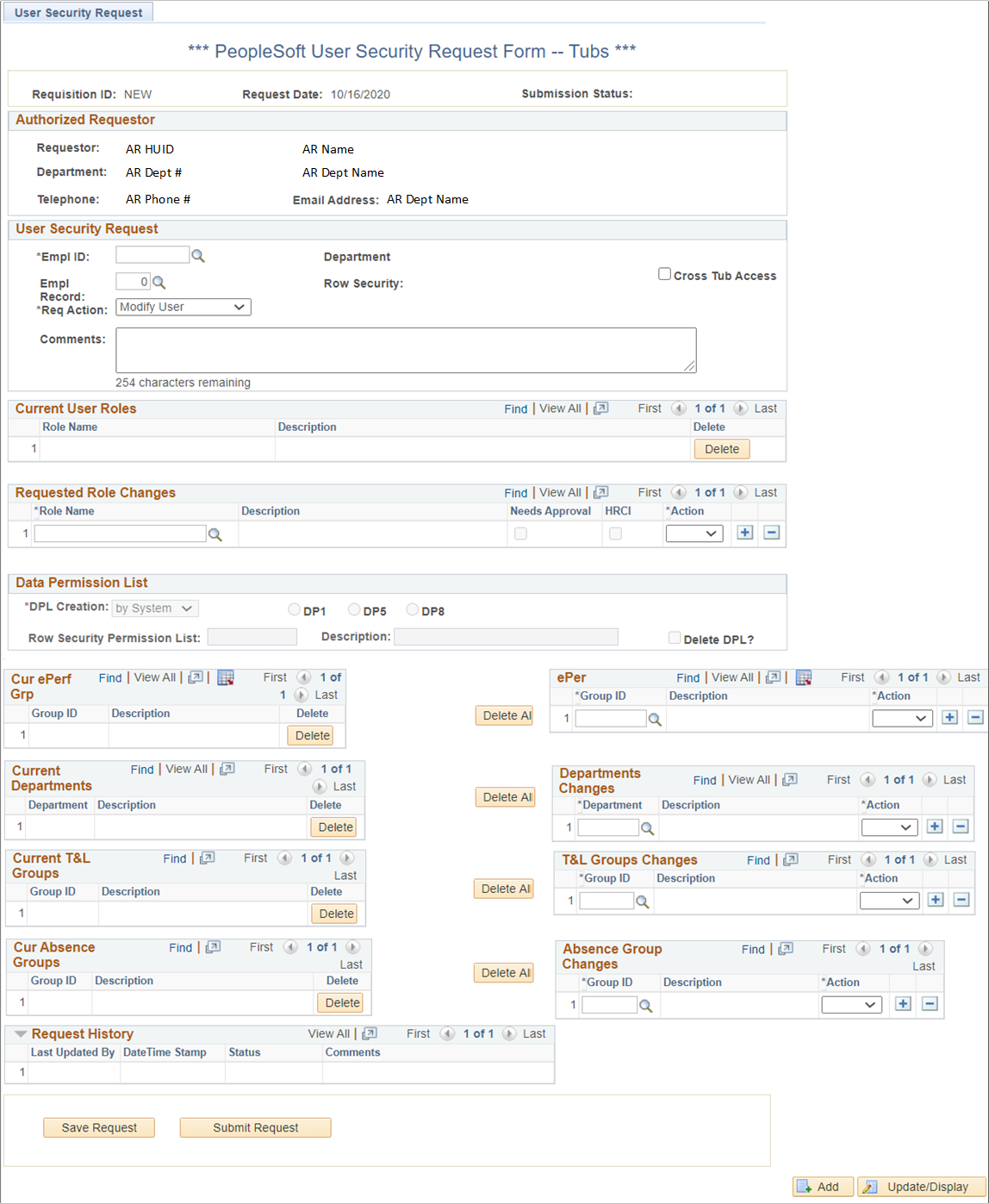


Screenshot 1, Find or Add a Value (Request)

Click the **Add a New Value** tab. Once in the **Add a New Value** select the **Add** button and a new request is opened.



Screenshot 2, Add a New Value (Request)



Screenshot 3, A New Request Opened in the PeopleSoft User Security Request Form

The new request will show all the various sections of the form. Some sections are automatically maintained by the system as the request is created and modified, while other sections require your input. The same sections are displayed whether you are giving a new user access or modifying the access of an existing PeopleSoft user.

Here is a list of the sections in the form and each item in the list links to its respective section in this document. Until you are familiar with the form, read through each section. You will find it is in the User Security Request section where you identify key detail about your request and determines the path for your request.

* [Requisition](#_Requisition_Information)
* [Authorized Requestor](#_Authorized_Requestor_Information)
* [User Security Request](#_User_Security_Request)
* [Current User Roles](#_Current_User_Roles)
* [Requested Role Changes](#_Request_Role_Changes)
* [Data Permission List (DPL)](#_Current_ePerformance_Groups)
* [Current Group and Department Associations](#_Current_Group_and)
* [Requested Changes to Group and Department Associations](#_Requested_Changes_to)
* [Request History](#_Request_History_and)
* [Save and Submit A Request](#_Save_and_Submit)

## Requisition Information

The requisition information is the top section of the form and it is maintained by the system. It is described in the table below.

| Field Name | Description |
| --- | --- |
| Requisition ID | NEW shows here until you Save or Submit your request for the first time. During the first Save or Submit a system-generated Requisition ID is assigned and it will display here going forward. |
| Requisition Date | Date the request is created. |
| Submission Status | A new request that has not yet been Saved or Submitted will have a blank status. See the [Process Flow for a User Security Request](#_bookmark3) and [Request History and Status](#_Request_History_and) in this document for the possible statuses. |

## Authorized Requestor Information

The Authorized Requestor information is the second section of the form and it is maintained by the system. It is information about you, the AR. It is described in the table below.

| Field Name | Description |
| --- | --- |
| Requestor | HUID and Name of the AR |
| Department | Department Number and Department Name of the AR |
| Telephone | Telephone number of the AR |
| Email Address | Email address of the AR |

## User Security Request

The User Security Request section is where you identify the user whose access you want to change, and the Request Action you are using to make the change. You can also enter comments about the request in this section.

There are three possible Request Actions and each takes its own path. Here are the three actions and they link to their respective place in this document:

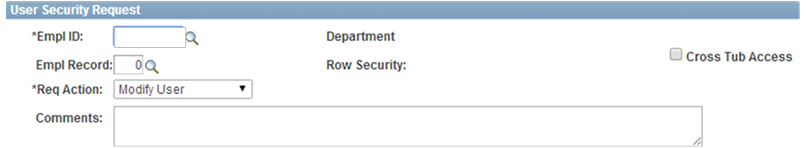
* [Modify User](#_Modify_User) - Add or delete user roles, departments, and groups.
* [Clone User](#_Clone_User) - Clone all items in one user's profile to another user.
* [Disable User](#_Disable_User) - Reduce a user's access to Basic and Self Service and delete all other roles. The user's groups and departments are deleted, including the Data Permissions List (DPL).

### Modify User

#### Identify User and Request Details

In the User Security Request section enter the user’s HUID in the Empl ID field. If a match is found, the person’s name will appear below the HUID you just entered. If it is the person you want, tab, or click, out of the field and the details about the user will populate the form. If it is not the person you want, or you want to search for the user, click on the magnifying glass to open the Look Up window.

Screenshot 4, User Security Request, Modify User



This table describes the fields of the User Security Request section when the Modify User Request Action has been selected:

| Field Name | Description |
| --- | --- |
| Empl ID | Required. The user’s HUID. As mentioned earlier, enter the ID or search for your user. See the [Look Up, Search](#_Look_Up,_Search) in this document for more information about the Look Up function. |
| Department | The user’s Department Number and Department Name displays after the Empl ID is identified. |
| Empl Record | For employees with multiple jobs, this is the Job Record to which the requested information pertains to. Record 0 is the default record but you can use the magnifying glass to look up the user’s jobs and select another record. |
| Row Security | The employee’s Data Permission List (DPL) displays. It shows the range of departments, and hence people, the user has access to. The DPL also includes the Time and Labor groups a user has access to, if any. It is maintained by Client Services based on your request, if you changed the departments or time and labor groups. |
| Cross Tub Access | Check this box if the user has multiple job responsibilities across Tubs. If checked, this box alerts Client Services to notify the AR of the cross Tub of the request. The AR in the cross Tub must approve the access to their Tub’s data. |
| Req Action | Required. This is the Request Action. Select Modify User. |
| Comments | Enter comments relevant to the request in the comments text box.  In addition, for Contingent Workforce (a.k.a. FieldGlass) you must enter the Tubs or Orgs for the Tub Owners and Orgs Owners in this comments text box. |

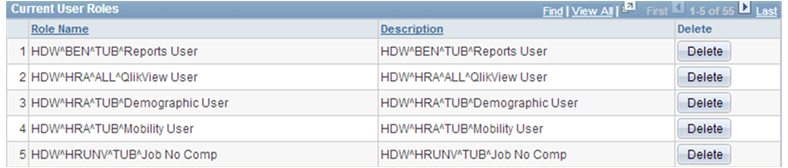
After entering and reviewing the User Security Request information you can make changes to roles and/or departments and/or groups:

* Go to the [Roles section](#_Roles) to review, add or remove roles.
* Go to the [Group and Department Associations](#_Group_and_Department) to review, add or remove group and department associations.

#### Roles

##### Current User Roles

A list of the roles currently assigned to the user are found in this section of the form. This section initially lists only five roles but it provides navigation to see more than five. The navigation elements are at the top right of the section. To learn more about the navigation go to the [Navigate List section in this document.](#_Navigate_Lists)



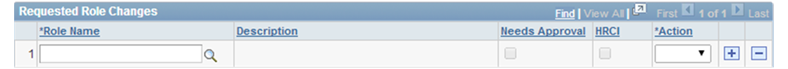
Screenshot 5, Current User Roles

For each role the following information displays:

| Column Name | Description |
| --- | --- |
| Row number | The list is numbered, starting with the number one. |
| Role Name | Roles already assigned to the user. |
| Description | The role description. It is often the same as the role name. |
| Delete | A delete button appears at the end of each row. Clicking on it places the role in the Requested Role Changes section for this request. |

##### Requested Role Changes

As you add or remove roles from a user’s profile the changes will accumulate in this section.



Screenshot 6, Requested Role Changes

For each role listed in the changes section the following information displays:

| Column Name | Description |
| --- | --- |
| Row number | The list is numbered, starting with the number one. |
| Role Name | The name of the role you are adding or removing. This is also where you would add a role. |
| Description | Same as the role name. |
| Needs Approval checkbox | The system will automatically check the checkbox if a role requires approval beyond the AR. Client Services will seek the approval after the HRAR submits the request. |
| HRCI checkbox | The system will automatically check the checkbox if a role has access to High-Risk Confidential Information, such as Social Security Numbers. |
| Action | The action you are performing with the role: Add or Delete. |
| + | Adds a row to this section. |
| - | Removes a row from this section. |

###### Delete a Role

To delete a role, click on the respective Delete button for the role in the Current User Roles section. The role will then appear in the Requested Role Changes section. The action type will default to Delete.

###### Add a Role

New roles are added in the Requested Role Changes section. A blank row is initially listed in that section and that is where you can add a role:

* Enter the role name and then tab out of the field or click in another field. If a valid role name was entered, the Description, Needs Approval and HRCI information will default into the row.
* If you do not know the role name, click on the magnifying glass to [look it up](#_Look_Up,_Search).
* The final step is select Add from the Action dropdown list.

If you need to add another role, click the plus sign on the right side of the last row and another row will be added for you.

#### Group and Department Associations

A user’s association to the following items can be changed:

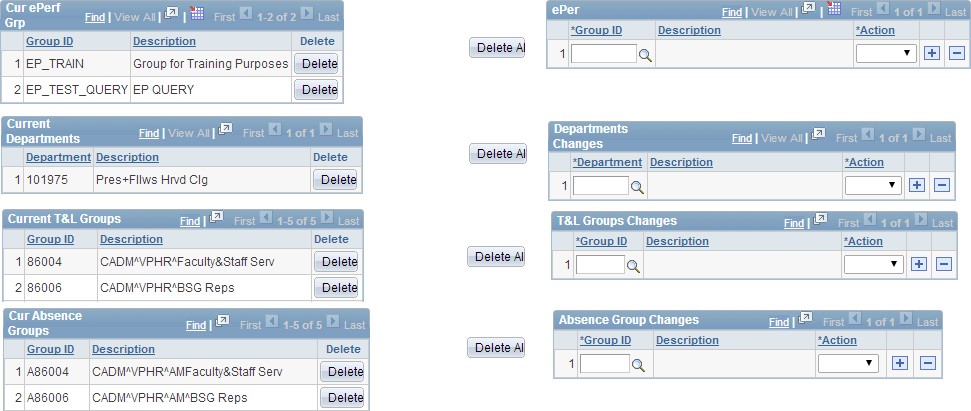
* ePerformance Groups
* Departments
* Time and Labor Groups
* Absence Groups

##### Data Permission List

This section is used only by Client Services. It is used to update the DPL if you make changes to the department and time and labor group associations.

##### Current Group and Department Associations

On the bottom half of the form is where you will find the department and groups a user is associated to. There are four kinds of associations and they appear in this order in the form: ePerformance Groups, Departments, Time and Labor Groups and Absence Groups. The current associations for the user are on the left side of the form while the changes requested are on the right side.



Screenshot 7, Group and Department Associations

The current associations will show the following details for each type:

| Column Name | Description |
| --- | --- |
| Row number | The list is numbered, starting with the number one. |
| ID | The ID number assigned to the current group or department. |
| Description | The name of the current group or department. |
| Delete | A delete button appears at the end of each row. Clicking on the button places the group or department in the respective changes section on the right. |
| Delete All | To the right of each list is a Delete All button. Clicking on the button places all associations for the group or department in the respective changes section on the right. |

##### Requested Group and Department Associations Changes

Across from the current associations are the changes you are requesting. As you add or delete an association the changes accumulate here. For each type of association, the following information displays:

| Column Name | Description |
| --- | --- |
| Row number | The list is numbered, starting with the number one. |
| ID | The ID number assigned to the group or department. |
| Description | The name of the group or department. |
| Action | The action you are performing for the group/department: Add or Delete. |
| + | Add a row to this section. |
| - | Remove a row from this section as well. |

###### Delete an Association

To remove an association from a user’s profile, click on the Delete button for group or department click the Current section. The group or department will then appear in the Changes section. The action type will default to Delete.

###### Add an Association

New group and department associations are added in the respective [Changes section](#_Requested_Changes), directly across from the current section for each group/department. Initially a blank row will be listed in that section and that is where you can add an association as follows:

* Enter the group or department ID and then tab out of the field or click in another field. The Description populates once the id is entered.
* If you do not know the ID, click on the magnifying glass to [look it up](#_Look_Up,_Search).
* The final step is select Add from the Action dropdown list.

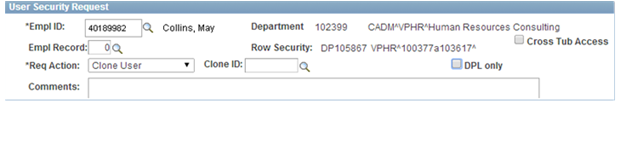
If you need to add another role, click the plus sign on the right side of the last row and another row will be added for you.

### Clone User

#### Clone Roles, Departments (DPL) and Groups

Clone User is an alternative to Modify User. It is its own type of request where you can assign roles and groups and departments by cloning the items in one user’s profile and giving them to another user. The user receiving the cloned profile will lose their current access and receive the access of the other user.

Note that the User Security Request information for the Clone User Request Action, when compared to Modify User, has two additional fields: Clone ID and a DPL only checkbox. When the DPL Only option is selected not all information is cloned; see the [Clone only the DPL](#_Clone_only_the) section for more information about that option.



Screenshot 8, User Security Request, Clone User

Follow these steps to replace a user’s current roles, departments and groups, with the roles, departments and groups of another user. Note, there is a way to make modifications to the cloned information once it populates the form:

1. Open a [new request as described earlier in this document](#_Open_a_User).
2. The [Requisition Information](#_Requisition_Information) and [Authorized Request Information](#_Authorized_Requestor_Information) will default in as described earlier.
3. In the User Security Request section, enter the user’s HUID in the Empl ID field. If a match is found, the person’s name will appear below the HUID you just entered. If it is the person you want, tab, or click, out of the field and the details about the user will populate the form. If it is not the person you want, click on the magnifying glass to open the Look Up window field and search for them.
4. You should also review/change the Empl Record (Job) to make sure the right one is selected, check the Cross Tub checkbox if applicable, and enter your comments, if any.
5. Once the Empl ID is identified, details about the user’s current access populates the form. It is an opportunity for you to review the access before it is replaced.
6. Select Clone User in the Request Action dropdown list.
7. Enter, or look up, the HUID of the user whose profile will be cloned in the Clone ID field. Once you identify the Clone ID, the Requested Changes sections on the form update with the new access the user will receive. The user’s current access will still show on the form but it will be removed when the request is processed.
8. If you would like to modify the access that defaulted in from the Clone ID user, you can. In other words, if you want a user to have someone else’s profile with a couple exceptions, follow the steps here:
   1. Change the Request Action from Clone User to Modify User.
   2. The access that was cloned from the Clone ID user is now editable. You can add or remove the roles, departments or groups.
9. You can [Save or Submit](#_Saving_and_Submitting) the request when you are ready.

The User Security Request fields for the Clone User Request Action are described in this table:

| Field Name | Description |
| --- | --- |
| Empl ID | Required. The user’s HUID. Enter the ID and then tab out of the field, or search for your user. See the [Look Up, Search](#_Look_Up,_Search) in this document for more information about the Look Up function. |
| Department | The user’s Department Number and Department shows once the Empl ID is identified. |
| Empl Record | For employees with multiple jobs, this is the Job Record to which the requested information pertains to. Record 0 is the default but you can use the magnifying glass to look up jobs and select another record. |
| Row Security | The employee’s Data Permission List (DPL) information. The DPL is a range of the departments, and hence the employees in those departments, to which the user has access to in PeopleSoft. It also includes time and labor groups. It is maintained by Client Services based on your request, if you change the departments or time and labor groups. |
| Cross Tub Access | Check this box if the user has multiple job responsibilities across TUBs. If checked, this box alerts Client Services to notify the AR of the cross Tub of the request. The AR in the cross tub must approve the access to their Tub’s data. |
| Req Action | Required. This is the Request Action. Select Clone User. |
| Clone ID | This is the HUID of user whose access will be cloned, duplicated, and assigned to the user identified in the Empl ID field. Once you identify the Clone ID in the form, the roles, groups, and department of the Clone ID displays. |
| DPL Only checkbox | If you want to clone only the DPL (Departments and/or Time and Labor Groups), check the DPL only box. The other information for the Empl ID will remain as is but you will have the option to edit it when you check this checkbox. |
| Comments | Enter comments relevant to the request in the comments text box.  Note, if the user is receiving the Tub Owner or Org Owner role for Contingent Workforce (a.k.a. FieldGlass), you must enter the Tubs or Orgs for the roles in this comments text box. Take this out or say only one can be the owner. |

#### Clone DPL Only

Selecting the DPL only checkbox clones only the Row Security Permission of the Clone ID user. It keeps the roles and group/department associations of the Empl ID user, but it lets you change their Current Roles or Absence Groups as part of the request. See Modify User to for help changing the [roles](#_Requested_Role_Changes_1) or [absence groups](#_Requested_Changes_to).

### Disable User

The Disable User Request Action reduces a user’s access to Basic and Self Service. All other roles are deleted along with the user’s DPL as well as any e-Performance groups, Departments, T&L Groups and Absence Groups. You cannot adjust a user’s access when choosing this action; all fields and options are disabled.

Follow these steps for the Disable User Request Action:

1. Open a [new request as described earlier in this document](#_Open_a_User).
2. The [Requisition Information](#_Requisition_Information) and [Authorized Request Information](#_Authorized_Requestor_Information) will default in as described earlier.
3. In the User Security Request section:
   1. Enter the HUID of the user in the Empl ID field or use the [Lookup/Search described earlier](#_Look_Up,_Search).
   2. Once the Empl ID is identified, details about the user’s current access populates the form. Review the information to be sure it is the user.
   3. Select Disable User for the Request Action.
   4. If you would like to enter comments you may.
4. [Save or Submit](#_Saving_and_Submitting) the request when ready.

# Save and Submit a Request

The Save and Submit Request buttons display for a new request, and additional buttons display after the request is initially Saved and/or Submitted.

1. Click the Save Request button. You will receive a confirmation message of the save; click on the OK button on the message. This option saves the request for you to return to it later and complete and/or submit it.
2. After you save a request, you also have the option to cancel the request by clicking the Cancel Request button. You will receive a confirmation message of the cancel; click on the OK button on the message.
3. When you are ready to submit the request to Client Services for processing, click the Submit Request button. You will receive a confirmation message of the submission; click OK on the message. Your request will be processed within 3-5 business days. You will receive an email notifying you of the status of your submission.
4. After you submit a request, you still have the option to cancel it by clicking on the Cancel Request button. You will receive a confirmation message of the cancellation; click OK on the message.

# Request History

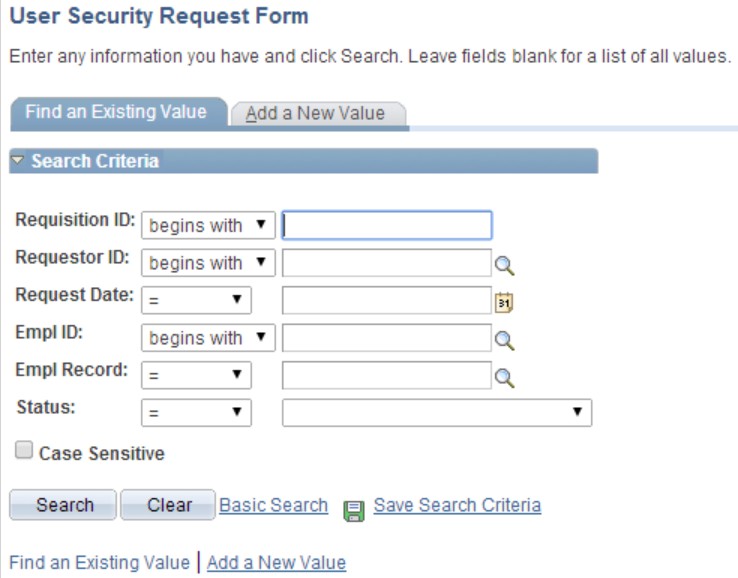
The Request History section contains a following information for each row of history, with the latest row on top:

| Field Name | Description |
| --- | --- |
| Last Updated By | Employee ID of the person who last updated the form |
| DateTime Stamp | Date and time the form was last updated |
| Status | A request can have one of the following statuses:   * Approved – Client Services approved request. * Cancelled – Client Services or the AR cancelled request. * Deleted – This status is not used. * Denied – This status is not used. * Processed: Client Services processed request (final action). * Rework: AR must rework. Resubmit request with required information described in the Comments field of the Request History section. * Saved: AR has saved, but not yet submitted, the request. * Submitted: AR has submitted request. * Submitted to HHR Reporting: Some roles automatically trigger this approval requirement. Client Services will wait for the approval before processing the request. |
| Comments | Comments entered Client Services. |

# Find an Existing Request

You will see only requests that you have created. To search for your requests navigate to the **Search Criteria** window as described in this document under [Navigate to the User Security Request Form](#_Navigate_to_the). You will arrive at the Find an Existing Value (Request) window. Select your search operator(s) and enter your search criteria; click on the Search button to get results.

Note, if you leave all the search fields blank and click on the Search button, the system will return all requests that you have created. Also note that you can only see requests that you have created. See the [Lookup/Search](#_Look_Up,_Search) to learn more about searches.



Screenshot 9, Find an Existing Value (Request)

# Have Questions?

Send your questions or concerns to the ATS Client Services email account: [fss\_client\_services@harvard.edu](mailto:fss_client_services@harvard.edu).