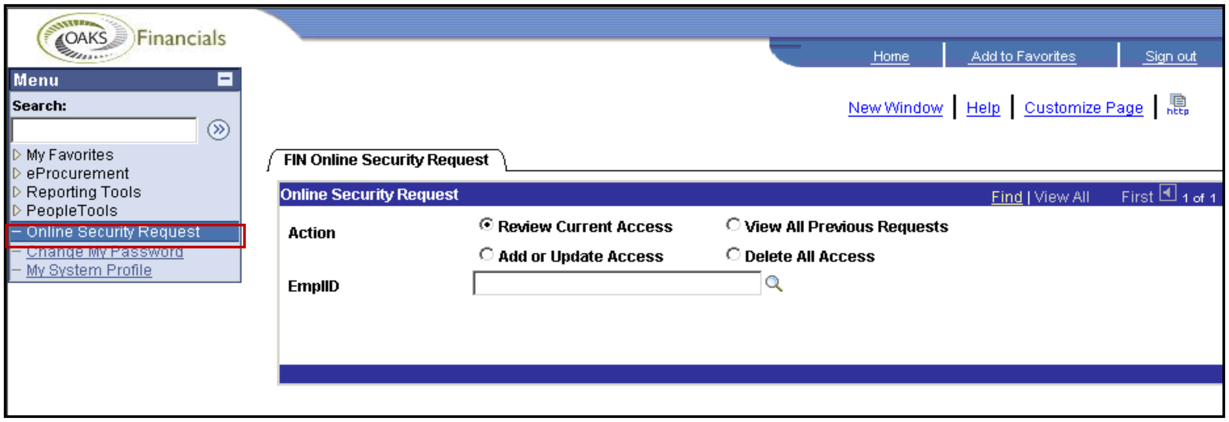
Purpose

The process of maintaining OAKS Financials security roles is done using the Ohio Administrative Knowledge System (OAKS) Financials (FIN) Online Security form located in the OAKS FIN application.

Navigation: Click on **Online Security Request** at the bottom of the Menu.



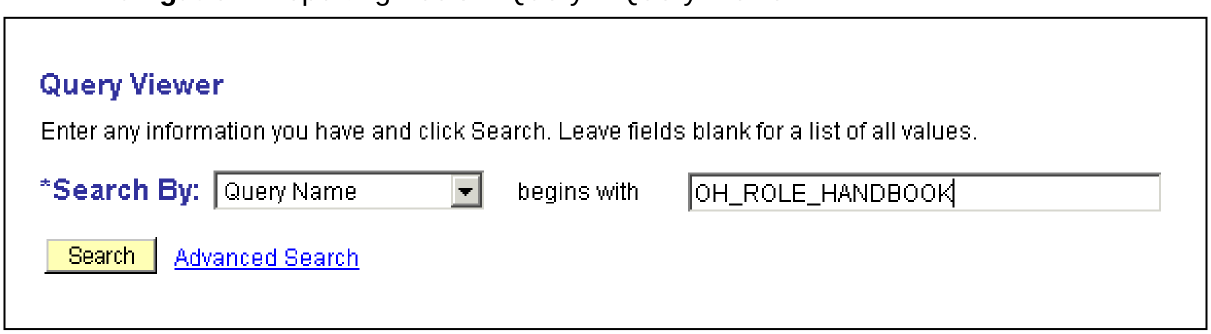
Reviewing, adding, updating, or deleting OAKS Financials user security roles

As the CFO or agency FIN Security Designee, it is your responsibility to review existing security roles, add new or update existing roles, delete old roles, and ensure that users of OAKS have the access they need to do their jobs and no more access than they need.

Best practice: Prior to entering the Online Security Request, review the information contained on the *Agency FIN Role Handbook* available in OAKS via the OH_ROLE_HANDBOOK query (both central and agency roles).

Agency FIN Security Designees can also view all user roles in their business unit(s) and the employees assigned to those roles using the OH_SEC_USER_ROLE_LISTING query.

Navigation: Reporting Tools > Query > Query Viewer



Access the Security Request Form

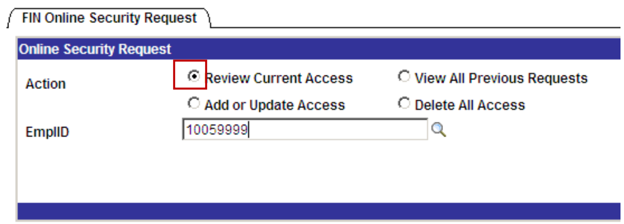
<table>
<tr><th>Step-by-Step</th><th>Screen</th></tr>
<tr><td>

1. Open the FIN Online Security Request Form in the OAKS FIN application.

2. Select an **Action** radio button to
   a. Review Current Access
   b. View All Previous Requests
   c. Add or Update Access
   d. Delete Access

3. Enter the Employee Identification Number (**EmplID**) and then press Enter on the keyboard.
   Or
   Use the look up icon 🔍 to find the ID

</td><td>

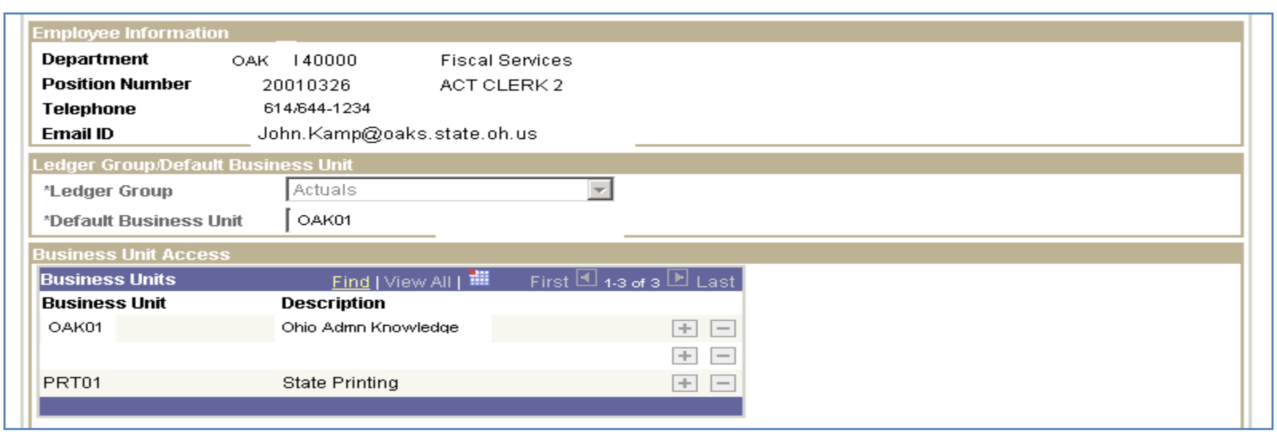


</td></tr>
</table>

Review Current Access

Employee Information, Ledger Group, and Business Unit Access appear at the top of the page. A list of all the security roles a user already has assigned will appear in the center of the page. Access Group, Voucher Processor Origin, and Purchasing Workflow information (if applicable) appear at the page bottom.

No changes can be made in this mode. If you determine you do need to add or update the information currently displayed for the user, your next step is to select the Add or Update Access radio button on the screen.



The middle of the screen shows the Role Assignments.

Role Assignment

Roles — Find | First 1-19 of 19 Last

Group Name	Add Role	Role Name	Description	Delete Role
AP - Accounts Payable	☐	OH_AP_PCARD_APPROVER	AP P-Card Approver	☐
AP - Accounts Payable	☐	OH_AP_PCARD_RECONCILER	AP P-Card Reconciler	☐
AP - Accounts Payable	☐	OH_AP_PCARD_VIEWER	AP P-Card Viewer	☐
AP - Accounts Payable	☐	OH_AP_REPORT_WRITER	AP Report Writer	☐
AP - Accounts Payable	☐	OH_AP_VENDOR_VIEWER	AP Vendor Viewer	☐
AP - Accounts Payable	☐	OH_AP_VOUCHER_MAINTAINER	AP Voucher Maintainer	☐
AP - Accounts Payable	☐	OH_AP_VOUCHER_PROCESSOR	AP Voucher Processor	☐
AP - Accounts Payable	☐	OH_AP_VOUCHER_VIEWER	AP Voucher Viewer	☐
AR - Accounts Receivable	☐	OH_AR_DEPOSIT_ORIGINATOR	AR Deposit Originator	☐
AR - Accounts Receivable	☐	OH_AR_VIEWER	AR Viewer	☐
Reporting	☐	OH_BURST_RL	Report Burster	☐
Reporting	☐	OH_EPM_CAS_LEGACY_WH_USER	EPM CAS Legacy Warehouse	☐
Reporting	☐	OH_EPM_COGNOS_PRIVATE	EPM Private Rpt Creator Cognos	☐
Reporting	☐	OH_EPM_QUERY_PRIVATE	EPM Private Query Creator	☐
GL - General Ledger	☐	OH_GL_VIEWER	GL - Viewer	☐
PO - Purchasing	☐	OH_PO_RECEIVING	PO - Receiver	☐
PO - Purchasing	☐	OH_PO_REQUESITIONER	PO - Requisitioner	☐
PO - Purchasing	☐	OH_PO_REQUESTOR	PO - Requestor	☐
PO - Purchasing	☐	OH_PO_VIEWER	PO - Viewer	☐

The bottom of the screen displays more details.

Access Group

Access Group: TECHADMIN

Accounts Payable Information

*Voucher Processor Origin: B80 — Ohio Administrative Knowledge

Purchasing Group Box

Purchasing Workflow IDs

Default Requestor: 10023456 — Mary Smith

*Next Level Approver ID: 10027890 — Kate Grand

Requestor Specific Information

Ship To Location: OAK01

Telephone:

Department:

ALI:

Fund Code:

Account:

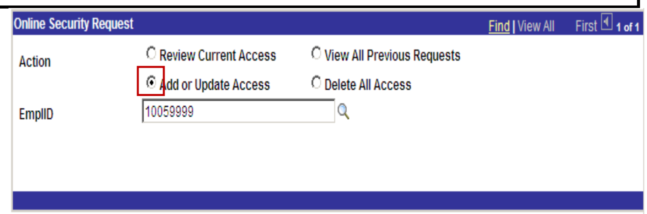
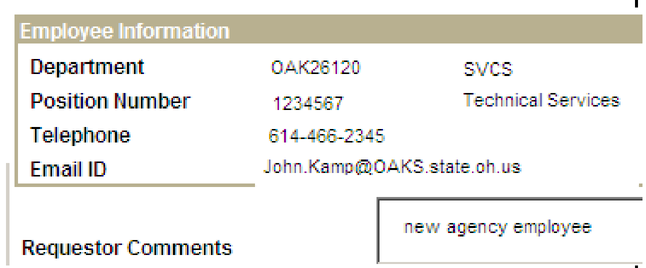
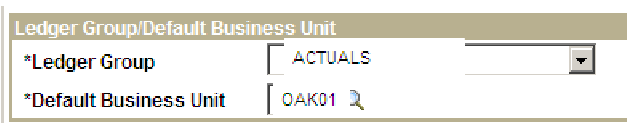
Program Code:

Add or Update Access

Employee Information, Ledger Group, and Business Unit Access appear at the top of the page. Below that, all the security roles a user already has assigned will appear at the top of a list and all additional roles available appear at the bottom of that list. Access Group, Voucher Processor Origin, and Purchasing Workflow information appear at the page bottom when applicable.

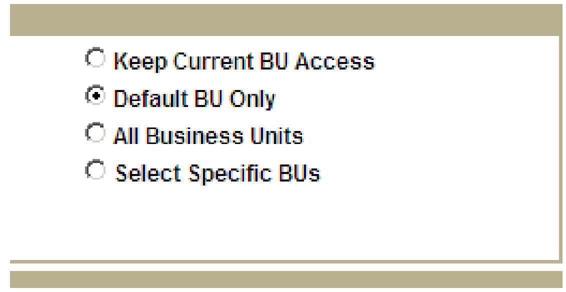
<u>All OAKS Financials access for the individual must be created or modified using this form</u>.

Add or Update Security Access

Step-by-Step	Screen
1. Return to the top of the page and select **Add or Update Access** as the Action.	
2. Verify the **Employee Information** populated is accurate. If there are errors, contact your agency HR department to update. 3. Enter a statement in the **Requestor Comments** field for record maintenance, and when applicable, add an explanation for the request when Central Approval is required.	
4. For **Ledger Group**, choose one: Actuals – All Agencies Full & Mod Accrual – OBM only Local (CFIS) – JFS only	
5. Enter the Primary agency Business Unit code for a new user. Verify the **Default Business Unit** appears when updating roles. 6. Click the Look up icon to confirm the Default Business Unit code.	

Note

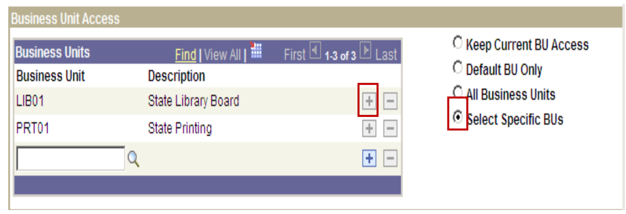
If this is a request for a user with no Default BU assigned prior to this request, a warning message will appear stating the business Unit Access will be marked as Default BU.



7. Select Specific BUs and click the + sign if you need to add additional Business Units.

Note

The Business Unit Access will always display the Default Business Unit and PRT01 (State Printing).



All Role Names will appear on the page in Group Name alphabetical order along with a short Description.

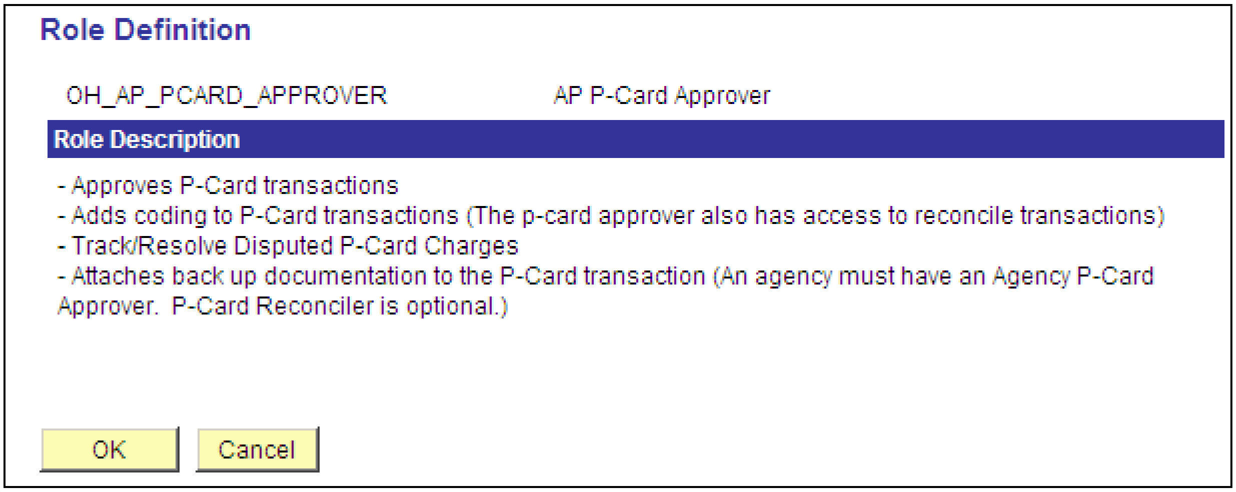
If you are adjusting access for an existing user, current roles are listed first, followed by all other roles available.

Role Assignment

Roles — Find | First 1-62 of 62 Last

Group Name	Add Role	Role Name	Description	Delete Role
AP - Accounts Payable		OH_AP_CONFIGURATION_PROCESSOR	AP Configuration Processor	
AP - Accounts Payable		OH_AP_JRNL_VOUCHER_PROCESSOR	AP Journal Voucher Processor	
AP - Accounts Payable		OH_AP_PCARD_APPROVER	AP P-Card Approver	
AP - Accounts Payable		OH_AP_PCARD_RECONCILER	AP P-Card Reconciler	
AP - Accounts Payable		OH_AP_PCARD_VIEWER	AP P-Card Viewer	
AP - Accounts Payable		OH_AP_REPORT_WRITER	AP Report Writer	
AP - Accounts Payable		OH_AP_VENDOR_VIEWER	AP Vendor Viewer	
AP - Accounts Payable		OH_AP_VOUCHER_VIEWER	AP Voucher Viewer	
AM - Asset Management		OH_AM_ASSET_ADJ_TRF_PROCESSOR	Asset Adjust/Trans Processor	
AM - Asset Management		OH_AM_ASSET_MAINT_PROCESSOR	Asset Maintenance Processor	
AM - Asset Management		OH_AM_ASSET_PROCESSOR	Asset Processor	
AM - Asset Management		OH_AM_ASSET_RETIRE_PROCESSOR	Asset Retirement Processor	
AM - Asset Management		OH_AM_ASSET_VIEWER	Asset Viewer	
AP - Accounts Payable		OH_AP_1099S_PROCESSOR	AP 1099S Processor	
AP - Accounts Payable		OH_AP_APPROVER_LEVEL1	AP Voucher Approver - Level 1	
AP - Accounts Payable		OH_AP_APPROVER_LEVEL2	AP Voucher Approver - Level 2	

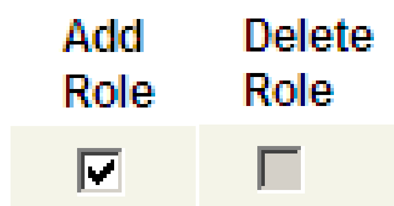
The Role Definition appears when you click on the Role Name link.



8. Click in the appropriate **Add Role** or **Delete Role** box to make adjustments. Do nothing to mark current roles that should remain active.

Note

You are not able to mark a box that is grayed out. That would mean you are trying to delete a role the user does not have or add a role the user already has assigned.



9. Choose an **Access Group** name to determine the time of day OAKS Financials will be available to the user.

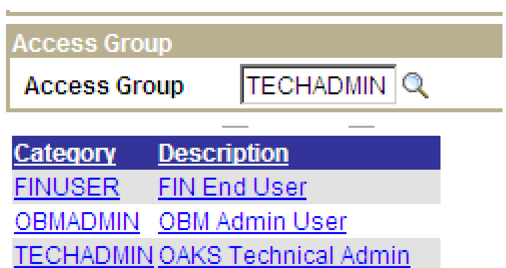
    a. FINUSER = 6 am – midnight, Mon-Sat

    b. OBMADMN = 7 days, 24 hours, and rights to keep normal access during year-end processing

    c. TECHADMN = 7 days, 24 hours

Note

Anything other than FINUSER will require central approval.



10. Press the **Submit Request** button. Note: A Warning message will appear asking the preparer to review the request. (Only the roles added or deleted will appear for review.)	Submit Request
11. After review, click either the **Finalize Request** button to submit, or **Modify Request** button to make adjustments.	Finalize Request Modify Request

Depending on the access requested, a warning may appear stating that the request has to be approved at the central level. You will receive e-mail notification when the request has been approved and processed or when it is denied.

Exceptions to immediate approval and access are:

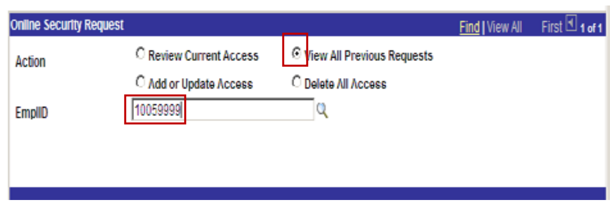
- Ledger type – Based on the Ledger Group selected by you
- Access Group – OBMADMN or TECHADMN selected for OAKS Category
- Business Unit – If you assign a Business Unit not in your Business Unit Profile
- GRF Access – Set to "Yes," approval must come from your agency security designee (Budget Planning Centers) and Central Agency approvers.

If central approval is not required, your request will be processed and access will be immediately available to the employee. (Your agency may have additional internal requirements.)

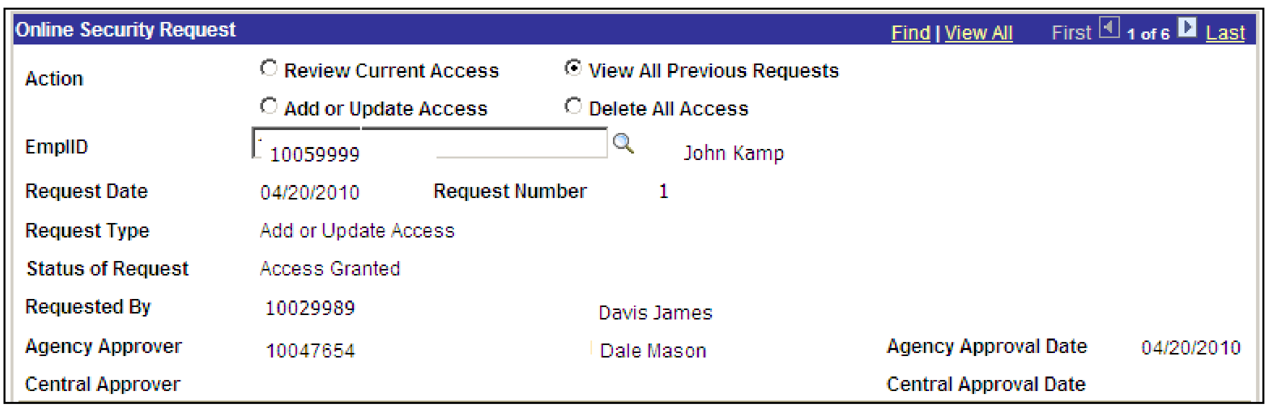
View All Previous Requests

Updates made for the user since online security go-live date will appear along with any comments.

View Previous Requests

Step-by-Step	Screen
1. At the top of the page select **View All Previous Requests** as the Action. 2. Enter the Employee Identification Number (**EmplID**) and then press Enter on the keyboard.	

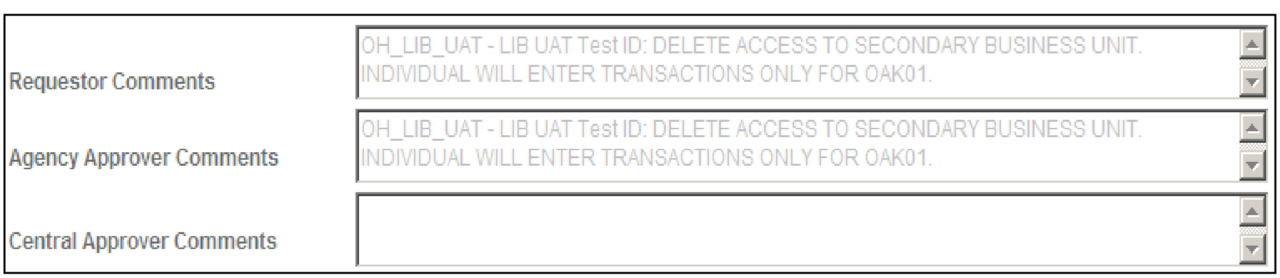
Approval information shows when the request was submitted, if status update has been granted or pending approval, who submitted the request, whether or not Central Approval was required, who approved the request, and when it was approved.



Online Security Request — Find | View All — First 1 of 6 Last

Action	Review Current Access / Add or Update Access	View All Previous Requests / Delete All Access	
EmplID	10059999	John Kamp	
Request Date	04/20/2010	Request Number	1
Request Type	Add or Update Access		
Status of Request	Access Granted		
Requested By	10029989	Davis James	
Agency Approver	10047654	Dale Mason	Agency Approval Date 04/20/2010
Central Approver			Central Approval Date

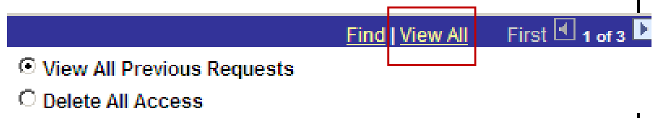
Comments from the requester and approver will appear if entered.



Requestor Comments	OH_LIB_UAT - LIB UAT Test ID: DELETE ACCESS TO SECONDARY BUSINESS UNIT. INDIVIDUAL WILL ENTER TRANSACTIONS ONLY FOR OAK01.
Agency Approver Comments	OH_LIB_UAT - LIB UAT Test ID: DELETE ACCESS TO SECONDARY BUSINESS UNIT. INDIVIDUAL WILL ENTER TRANSACTIONS ONLY FOR OAK01.
Central Approver Comments	

<table>
<tr>
<td>3. Click the View All link at the top of the page to review multiple updates (three per page).

Or

Click the forward  or backward  icon to view updates one at a time.</td>
<td>


</td>
</tr>
</table>

Delete All Access

All roles currently assigned to a FIN user are marked for deletion when submitted. Once finalized, roles will be deleted immediately and cannot be undone.

Delete Security Access

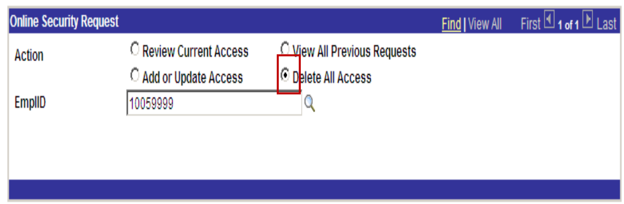
Step-by-Step

1. Select **Delete All Access** as the Action.
2. Enter the Employee Identification Number (**EmplID**) and then press Enter on the keyboard.

   Or

   Use the look up icon to find the ID.

Screen



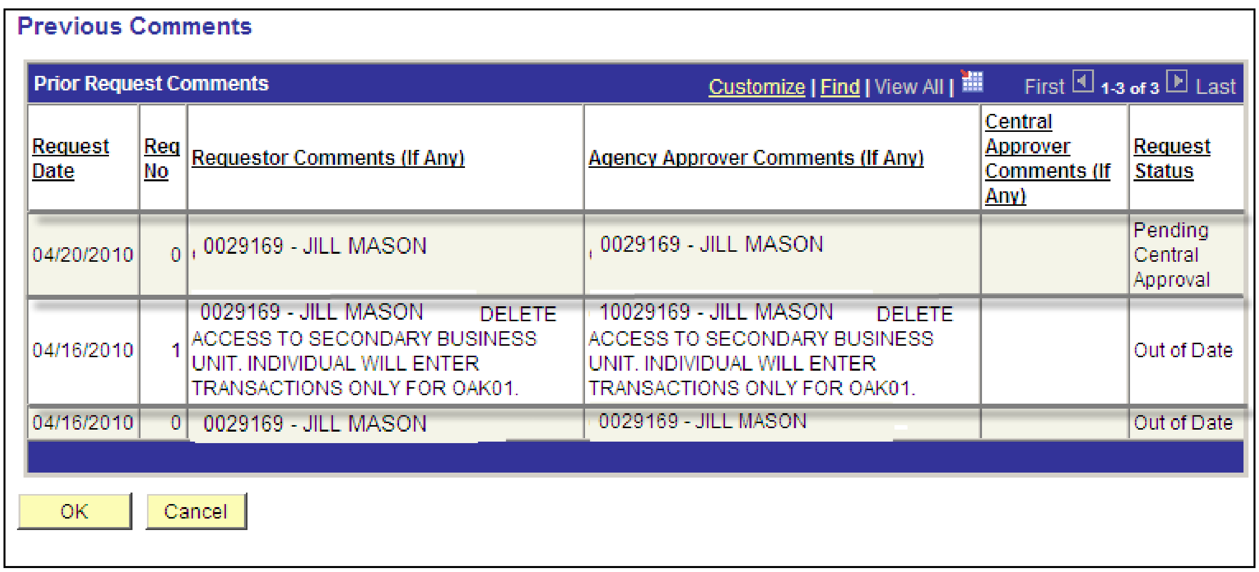
Step-by-Step

OPTIONAL

Click the **Previous Request Comments** link to view prior requests for security updates for the user along with any comments.

Screen

The previous comments will display.



Previous Comments

Prior Request Comments — Customize | Find | View All | First 1-3 of 3 Last

Request Date	Req No	Requestor Comments (If Any)	Agency Approver Comments (If Any)	Central Approver Comments (If Any)	Request Status
04/20/2010	0	0029169 - JILL MASON	0029169 - JILL MASON		Pending Central Approval
04/16/2010	1	0029169 - JILL MASON DELETE ACCESS TO SECONDARY BUSINESS UNIT. INDIVIDUAL WILL ENTER TRANSACTIONS ONLY FOR OAK01.	10029169 - JILL MASON DELETE ACCESS TO SECONDARY BUSINESS UNIT. INDIVIDUAL WILL ENTER TRANSACTIONS ONLY FOR OAK01.		Out of Date
04/16/2010	0	0029169 - JILL MASON	0029169 - JILL MASON		Out of Date

OK Cancel

Click OK to close.

FIN Agency Security Online Request

View the status of a prior change request that has not been processed and any related comments from the requestor.

Prior Request Status	Prior request for user made on 2010-04-20 has not yet been fully processed. That request is 'Pending', and is still in the process of being approved. If you complete a new request the old request will be cancelled and replaced by this request
Requestor Comments	

All current security roles are listed and are marked to delete.

Group Name	Add Role	Role Name	Description	Delete Role
AP - Accounts Payable	☐	OH_AP_PCARD_APPROVER	AP P-Card Approver	☑
AP - Accounts Payable	☐	OH_AP_PCARD_RECONCILER	AP P-Card Reconciler	☑
AP - Accounts Payable	☐	OH_AP_PCARD_VIEWER	AP P-Card Viewer	☑
AP - Accounts Payable	☐	OH_AP_REPORT_WRITER	AP Report Writer	☑
AP - Accounts Payable	☐	OH_AP_VENDOR_VIEWER	AP Vendor Viewer	☑
AP - Accounts Payable	☐	OH_AP_VOUCHER_PROCESSOR	AP Voucher Processor	☑
AP - Accounts Payable	☐	OH_AP_VOUCHER_VIEWER	AP Voucher Viewer	☑
AR - Accounts Receivable	☐	OH_AR_DEPOSIT_ORIGINATOR	AR Deposit Originator	☑
AR - Accounts Receivable	☐	OH_AR_VIEWER	AR Viewer	☑
Reporting	☐	OH_BURST_RL	Report Burster	☑

You will receive an error message when trying to delete all FIN roles if that user has a workflow approval role with no other user assigned to that BU/Origin for approval.

Windows Internet Explorer

You cannot delete the OH_AP_APPROVER_LEVEL1 role from your profile as there is no other user assigned to Approve the following BUs/Origins. Please make sure another employee is assigned to these BUs/Origins and then you can remove this role from the current employee.

B80_Origin (0,0)

OK

To remove all non-workflow related roles, choose the **Add or Update Access** mode to delete only select roles. Once the workflow team cleans up the remaining issues the Agency Security Designee can go back into **Delete All Access** mode to finish removing that user's remaining access.

Contact the OAKS Helpdesk at OAKS.Helpdesk@oaks.state.oh.us to create a ticket for the PO-RACM Purchasing Team when there are outstanding worklist items and have them appropriately transferred, closed, deleted, etc.

3. Click the **Submit Request** button at the bottom of the page.	Submit Request
A warning message appears asking you to review the request and verify you truly want the individual to have their access fully revoked.	
4. Click the **OK** button to confirm the request.	OK
5. Click the **Finalize Request** button to revoke all access for the employee. Or Click the **Modify Request** button to make changes.	Finalize Request Modify Request
6. Press the **Submit Request** button.	Submit Request

A message will appear stating the request to delete all FIN access is approved and granted.