

Secondary Security Administrator's Guide

General Information

Secondary Security is a Human Resources' (HR) tool that is used to manage access to a variety of online applications. Examples include, but are not limited to, AP-PO, Cash Handling, Effort Reporting, General Ledger Decision Support System (GL DSS), Grant DSS, HR Reporting, HR Transaction System and Time Reporting.

This tool is used and managed at the ORG or DEPT level. Once an employee is given access to an application which uses Secondary Security, she/he is immediately able to use that application; there are no central University forms to be completed, no Workflow approvals required and no waiting period. Any approval processes desired are created and administered internally and independently by ORGs or DEPTs across campus.

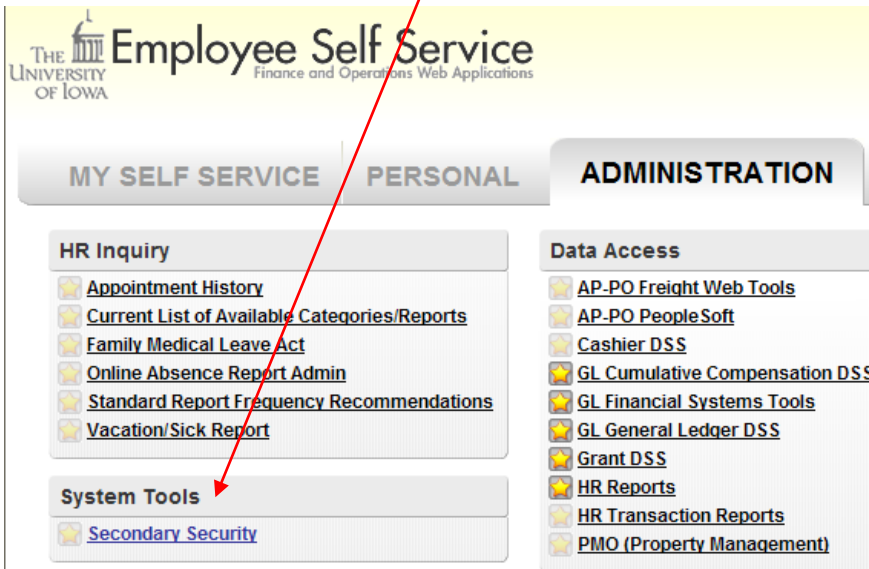
This administrator's guide was created and is maintained by Accounting and Financial Reporting with the intent to assist those who need to use Secondary Security in conjunction with online Accounting and Financial Reporting's applications. It has been purposely kept somewhat general in nature to address basic information that would apply in any situation; information specific to individual applications is included only for those owned and supported by Accounting and Financial Reporting. Currently GL DSS and Cash Handling are Accounting and Financial Reporting's only online applications which use Secondary Security. No attempt will be made to provide details specific to applications not owned and supported by Accounting and Financial Reporting.

Access Types

1. **ADMIN** access - A person with **ADMIN** access can grant either **ADMIN** or **WORK** access to someone else. Only those people with **ADMIN** access can see or use the Secondary Security tool.
2. **WORK** access - A person with **WORK** access can use the target application (e.g. GL DSS).

Signing In

Secondary Security is located in Employee Self Service, ADMINISTRATION tab, System Tools section. This link will be seen only by people who already have ADMIN access for at least one application that uses Secondary Security. <https://hris.uiowa.edu/portal/>



The screenshot displays the 'Employee Self Service' portal interface. At the top, the University of Iowa logo and the text 'Employee Self Service Finance and Operations Web Applications' are visible. Below this, there are three main navigation tabs: 'MY SELF SERVICE', 'PERSONAL', and 'ADMINISTRATION'. The 'ADMINISTRATION' tab is currently selected. Underneath the tabs, there are two main sections: 'HR Inquiry' and 'System Tools'. The 'System Tools' section contains a link for 'Secondary Security'. A red arrow points from the URL in the text above to the 'Secondary Security' link in the screenshot.

MY SELF SERVICE	PERSONAL	ADMINISTRATION
HR Inquiry <ul style="list-style-type: none">Appointment HistoryCurrent List of Available Categories/ReportsFamily Medical Leave ActOnline Absence Report AdminStandard Report Frequency RecommendationsVacation/Sick Report		Data Access <ul style="list-style-type: none">AP-PO Freight Web ToolsAP-PO PeopleSoftCashier DSSGL Cumulative Compensation DSSGL Financial Systems ToolsGL General Ledger DSSGrant DSSHR ReportsHR Transaction ReportsPMO (Property Management)
System Tools <ul style="list-style-type: none">Secondary Security		

Using Secondary Security

- 1) From the drop-down menu, select the target application – the application you want to grant access for.
- 2) Enter one of the identifiers of the person you want to grant access to.

Secondary Security Authorization

Select from the fields below and click Continue.



**For access to secondary applications, an individual must have access to HR Self Service.
 For access to HR-Related secondary applications, an individual must have access to the HR Data Access Applications.**

- This application allows you to manage security for other employees to secondary applications such as the Graduate Reappointment Application and AP/PO PeopleSoft Web Applications.
- You will be granting/removing security only for those orgs/departments that you select on the following screen.
- Please select the Employee and Application for whom you wish to authorize security.

APPLICATION: v
 EMPLID:
 SSN:
 LAST NAME:
 FIRST NAME:

- 3) Select the correct person if there is more than one possible match.

You are here: [Administration](#) » [Secondary Security Authorization](#) » [Select Employee](#)

Select Employee

Please choose an employee from the following list. If you do not wish to choose one of the following employees, return to the [main Secondary Security Application page](#).

EMPLID	NAME	SSN	DEPTID	JOBCODE
<input checked="" type="radio"/> 1014253	GRITTON,CAROLYN KOHL	***-**-2861	05-0305	PB30
<input type="radio"/> 1107267	GRITTON,JASON MATTHEW	***-**-1635	49-4655	S310
<input type="radio"/> 1011317	GRITTON,JOANNE MARY	***-**-0658	70-7650	GB32
<input type="radio"/> 1069896	GRITTON,KATHERINE M	***-**-6243	49-4756	S150
<input type="radio"/> 1098322	GRITTON,LACI JILLIAN	***-**-8561	49-4756	S150
<input type="radio"/> 1063143	GRITTON,LORI KATHLEEN	***-**-5661	70-7280	GB12

Secondary Security Administrator's Guide

4) Grant either ADMIN or WORK access by selecting the appropriate radio buttons. Scroll down to find applicable ORGs and DEPTs and make the selections.

Authorize Access for GRITTON,CAROLYN KOHL

☺ CHOOSE APPLICATION

Application Name: GLDSS ▾ Change

☺ CURRENT APPLICATION: GLDSS

You may add or remove security authorization by selecting the appropriate radio button for that unit.

- **Work Access** - indicates that an individual can use the application for that unit.
- **Admin Access** - indicates that an individual can not only use the application for that unit, but can also authorize others to use the application.

ORG 01	<input type="radio"/>	ADMIN ACCESS	<input type="radio"/>	WORK ACCESS	<input checked="" type="radio"/>	NO ACCESS
DEPT 01-0001	<input type="radio"/>	ADMIN ACCESS	<input type="radio"/>	WORK ACCESS	<input checked="" type="radio"/>	NO ACCESS
DEPT 01-0030	<input type="radio"/>	ADMIN ACCESS	<input type="radio"/>	WORK ACCESS	<input checked="" type="radio"/>	NO ACCESS
DEPT 01-0035	<input type="radio"/>	ADMIN ACCESS	<input type="radio"/>	WORK ACCESS	<input checked="" type="radio"/>	NO ACCESS
DEPT 01-0050	<input type="radio"/>	ADMIN ACCESS	<input type="radio"/>	WORK ACCESS	<input checked="" type="radio"/>	NO ACCESS
DEPT 01-0055	<input type="radio"/>	ADMIN ACCESS	<input type="radio"/>	WORK ACCESS	<input checked="" type="radio"/>	NO ACCESS
DEPT 01-0060	<input type="radio"/>	ADMIN ACCESS	<input type="radio"/>	WORK ACCESS	<input checked="" type="radio"/>	NO ACCESS
DEPT 01-0180	<input type="radio"/>	ADMIN ACCESS	<input type="radio"/>	WORK ACCESS	<input checked="" type="radio"/>	NO ACCESS
DEPT 01-0317	<input type="radio"/>	ADMIN ACCESS	<input type="radio"/>	WORK ACCESS	<input checked="" type="radio"/>	NO ACCESS
DEPT 01-4630	<input type="radio"/>	ADMIN ACCESS	<input type="radio"/>	WORK ACCESS	<input checked="" type="radio"/>	NO ACCESS

Both types of access can be granted at a total ORG level or an ORG-DEPT level. For most applications, this differentiation only has meaning for ADMIN access.

If a person has ADMIN access at an ORG level, she/he can give other people ADMIN access to that **same** ORG or to any specific DEPT within that ORG. If a person has ADMIN access to one or more specific DEPTs within an ORG, she/he can give other people ADMIN access to any of those **same** DEPTs within that ORG.

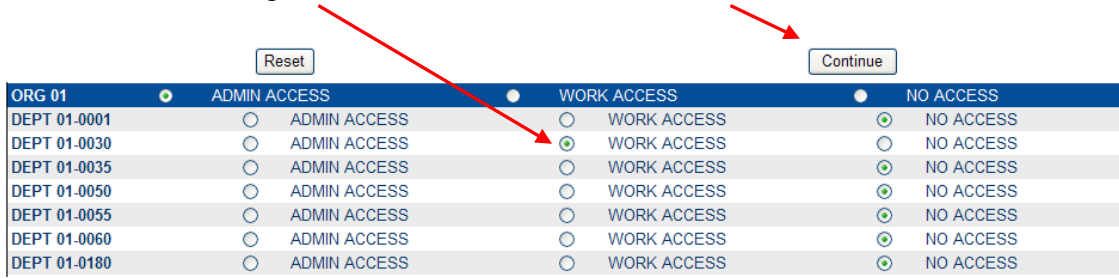
An ADMIN cannot grant either type of access outside of the ORG or ORG-DEPT that they have been set up for.

For a person to be able to use the GL DSS application (WORK access only), it is necessary to ONLY grant that person WORK access for a single DEPT or at the ORG level with no specific departments selected. It is NOT necessary to set that person up with WORK access to multiple departments and not advisable to do so because it creates unnecessary records; the extra records make the HR Secondary Security reports more difficult to use. For example, if a person needs the ability to review GL DSS online reports for departments 0001, 0030, 0035 and 0060, it is only necessary to select ONE of those departments when granting WORK access.

Secondary Security Administrator's Guide

For applications other than GL DSS, check with the application owner to see if there is additional security tied to setting a person up for multiple departments or multiple organizational units.

After the desired assignments are made, select the "Continue" button to make the selections effective.



ORG 01	ADMIN ACCESS	WORK ACCESS	NO ACCESS
DEPT 01-0001	<input type="radio"/> ADMIN ACCESS	<input type="radio"/> WORK ACCESS	<input checked="" type="radio"/> NO ACCESS
DEPT 01-0030	<input type="radio"/> ADMIN ACCESS	<input checked="" type="radio"/> WORK ACCESS	<input type="radio"/> NO ACCESS
DEPT 01-0035	<input type="radio"/> ADMIN ACCESS	<input type="radio"/> WORK ACCESS	<input checked="" type="radio"/> NO ACCESS
DEPT 01-0050	<input type="radio"/> ADMIN ACCESS	<input type="radio"/> WORK ACCESS	<input checked="" type="radio"/> NO ACCESS
DEPT 01-0055	<input type="radio"/> ADMIN ACCESS	<input type="radio"/> WORK ACCESS	<input checked="" type="radio"/> NO ACCESS
DEPT 01-0060	<input type="radio"/> ADMIN ACCESS	<input type="radio"/> WORK ACCESS	<input checked="" type="radio"/> NO ACCESS
DEPT 01-0180	<input type="radio"/> ADMIN ACCESS	<input type="radio"/> WORK ACCESS	<input checked="" type="radio"/> NO ACCESS

You will then be returned to the Secondary Security Authorization main screen where you can select another person and/or application. Access is granted to one person and one application at a time.

Revoking Access

Termination:

Information Management Finance and Operations (IMFO, a department of HR) runs a job daily which looks for terminations in HR appointments. Based on the termination effective date, this job automatically removes all Secondary Security records for that employee. This is true regardless of the application(s) the person has access to and the type of access granted. No email notifications are sent.

There is an exception to this process: if an employee has multiple appointments in the HR system, ALL appointments must be terminated in order for the revocation job to remove his/her Secondary Security records. If one appointment is still active in HR, then an automatic revocation will NOT occur.

Transfer:

IMFO, on behalf of Accounting and Financial Reporting runs a job daily which looks for employee transfers and revokes Secondary Security access accordingly. A **transfer** is defined in this situation as a **change in both DEPT and position number for the person's primary appointment**, as recorded in the HR system. This transfer data is collected for those people who have Secondary Security access to the **GL DSS** online reporting application (listed as GLDSS in Secondary Security). *Other applications may or may not have transfers monitored in a similar way.*

Secondary Security Administrator's Guide

This job runs each morning at 6:15. When a transfer condition is found with an effective date of “today,” all of that person’s Secondary Security records for **GL DSS** are deleted, which revokes his/her access to this application. Email notifications of this action are sent to the person who had access revoked and to the Secondary Security administrators of both the former position and the new position. Only Secondary Security DEPT administrators receive the emails. If there are no specific affected DEPT admins, then all ORG admins for the ORG in question will receive the emails. If the person transferring needs to have access to the GL DSS application in the new position, a Secondary Security admin in the new work area will need to grant the person access.

Manually revoking access:

When an ORG or ORG-DEPT admin must revoke access because there is no automated process in place (or for other reasons), this is done in the same way that access is granted – only in reverse. Sign into Secondary Security and one person and one application at a time, **un-select** all applicable buttons for WORK and ADMIN access being revoked.

Secondary Security Administrator responsibilities:

When an employee with one HR appointment terminates, access revocation is automatic and the ORG and ORG-DEPT admins do not need to take any action.

If an employee has multiple appointments and the ORG or ORG-DEPT admin determines Secondary Security should be revoked, then the admin will need to revoke access to all applications.

When an employee transfers, the ORG or ORG-DEPT admin

- for the position the employee is **leaving**
 - does NOT need to revoke access for GL DSS
 - MAY need to revoke access for applications other than GL DSS
- for the position the employee is **going to**
 - DOES need to set the employee up for any Secondary Security applications the employee will need to use in the new position

Secondary Security Help

If you have questions about who already has ADMIN or WORK access for a given application, there are HR reports which can provide that information. They are available through Self Service, assuming you have the proper HR security level to view these reports. Follow this navigation:

Self Service → ADMINISTRATION tab → HR Reports link → Security Reports link

[Secondary Security - Dept/App](#)

List of employees security by application and department.

[Secondary Security by App](#)

List of employees security by application.

[Secondary Security by Dept](#)

List of employees with security to Secondary Applications within a given department.

[Secondary Security by Employee](#)

List of secondary applications to which a given employee has access.

Because Secondary Security is a generic tool that is used for many applications across various business units, questions about how to use Secondary Security should be addressed to the owner of the application you are using Secondary Security for. For example, if you need to use Secondary Security for an application that Accounting and Financial Reporting owns, such as GL DSS or Cash Handling, direct your questions to your Accounting and Financial Reporting ORG contact. The ORG contact list (<http://www.uiowa.edu/~fusas/contact.html#staff>) is found on the front page of the Accounting and Financial Reporting website (<http://www.uiowa.edu/~fusas/>). Questions can also be sent to the Accounting and Financial Reporting email account: accounting-services@uiowa.edu.

Secondary Security Administrator's Guide

When in doubt about who to contact with questions, use the 'Contact Us' link at the top of any Employee Self Service page.



On the following screen, select the 'Other' category and write your comments. Make it clear that you are asking about 'Secondary Security' and include the application/system you need to use (e.g. AP-PO, Effort Reporting). Sending this form generates an email. Your question will be routed to someone who can assist you.

What is your question or comment in regards to? Carefully select from the list of choices below. Making the proper selection will help you get your question answered in the most efficient manner. If you're unsure, please select Other.

- Benefits (Flex Benefits, Spending Accounts, Beneficiaries, Retirement, Insurance)
- Compensation and Classification
- Employee Self Service Website
- E-Voucher
- Human Resources
- Payroll (Direct Deposit, Paycheck, Tax Withholding, Yearend Taxes)
- PReqs
- ProTrav
- Transaction System
- Workflow (Questions about establishing/maintaining Workflow paths)
- Other

Comments: (Please provide as much information as possible about your issue)

Summary

- Secondary Security is used by individual ORG/DEPT staff to give people in their areas access to selected online applications.
- WORK access allows a person to use the target application.
- ADMIN access allows a person to grant WORK or ADMIN access to other people.
- Secondary Security is found in Employee Self Service, ADMINISTRATION tab, System Tools section. Only those people with ADMIN access to at least one application will see the Secondary Security link.
- The drop-down menu of applications that a person sees contains only those applications that she/he has ADMIN access to.
- Access is granted to/revoked from one person and one application at a time.
- Granting WORK access to only a single department or single organizational unit is sufficient and preferred for **GL DSS**; it is not necessary to select multiple DEPTs within an ORG or multiple ORGs.
- ORG and ORG-DEPT administrators do not need to remove application access for **GL DSS** when a person transfers out of her/his department; GL DSS revokes are automatically done. Transfer revokes for other applications may or may not be automatic – this should be confirmed with the department that owns the individual application.
- Access is automatically removed for a person with one HR appointment when she/he terminates employment with the University. ORG and ORG-DEPT administrators should remove application access for all applications as appropriate for employees who have multiple appointments and one of those appointments has remained active in HR.
- Reports on who has access to which applications are available in HR Reports → Security Reports.