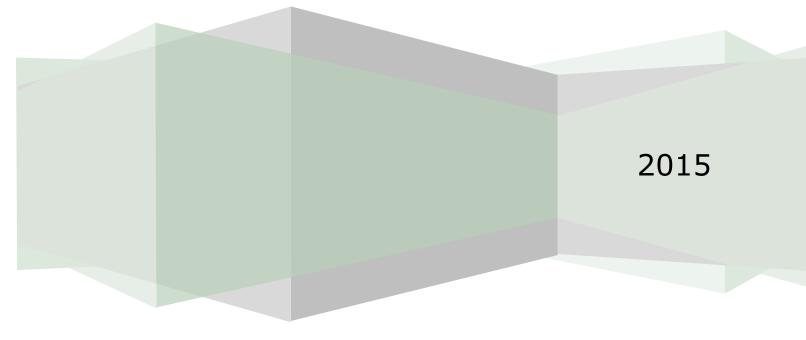


# Security Dashboard Users Guide

Security Admin Reports Security Analyzer Security Auditing Object Modeling Object Comparison Security Visualizer



# Contents

Introduction
Setting your Default Home Page6
Configuring your LDAP Reporting Profile
Security Admin Reports8Pre-Report Filters10Adding or Removing Selected Values12Adding or Dropping All Values13Adding or Removing Criteria Based Filters14Historical Comparisons15Changing Pre-Report Filters16Showing and Hiding Columns16On-The-Fly Report Filters18
Grouping.19Creating a Group19Grouping - Nested21Grouping - Expand, Collapse or Remove21Grouping - Remove Filters.22
Sorting22Adding a Sort Option22Removing the Sort Option23
Saving Security Reports
Running Saved Report 24
Exporting and Printing
Drilling
Reports List27Users27Roles27Tasks (Security Classes)27Ancillary Data28Listener28
Security Analyzer

Refreshing Your Data	30
Creating a New Report	30
Running an Saved Report	30
Editing a Saved Report	32
Deleting a Saved Report	. 32
Report Options	. 32
Reading the Analyzer Report	33
Users Assigned Roles	33
Assigned Forms	33
Assigned Roles and Security Classes	34
Assigned Form Conditions	
Assigned Tables	
Assigned Program Codes	
Assigned Fields	
Assigned Field Conditions	
Function Code Legend	35
Change Audit Reporting	36
Quick Search	
Advanced Search	
Prompt at Runtime	
Exporting	
Creating a MS Excel Document	
Creating a PDF	40
Printing	41
Saving a New Query	41
Saving an Existing Query	41
Scheduling Reports	42
Deleting a Report	43
Renaming a Report	43
Object Modeling	
Removing an Object Assignment from a ExistingTask	
Adding an Object to a New Task	
Changing a Forms Function Code Rule	
Linking to Security Reports	
Viewing potential Segregation of Duties violations	52
Role Modeling	54
Adding a Role to a User	54
	51
Object Comparison	
Comparing Roles-Tasks Assignments	
Comparing Roles-Tasks Assignments at the Object Level	59

Comparing Tasks Assignments Comparing Tasks Assignments at the Object Level	
Security Visualizer Displaying a User Map	
Settings	
Applying Filters to a User Map	
Modifying Role Assignments Modifying Security Class (Task) Assignments	
Clear Mapping	
Security Utilities	75
Trouble Shooting	77

# Introduction

The Kinsey LS Dashboard provides user friendly Lawson security administrator reports, security auditor reports and security change reports.

The security administrator reports are designed to help with the administration of Lawson Security queries showing detailed security information by User, Role and Security Class (Task) including all objects and rules.

The Security Analyzer report is specifically built as an audit tool to easily review access by user. The Microsoft Excel output makes it easy to analyze category, form, table, and field level security by user.

The Security Change Audit report provides details on changes made to your security model including who made the change, when it was made and the before and after values.

These independent queries have been designed to provide access to your data in the quickest most robust method possible through a browser interface. The Security Dashboard reports provide critical insight into your security model for your security administrators and your security auditors.

# **Setting your Default Home Page**

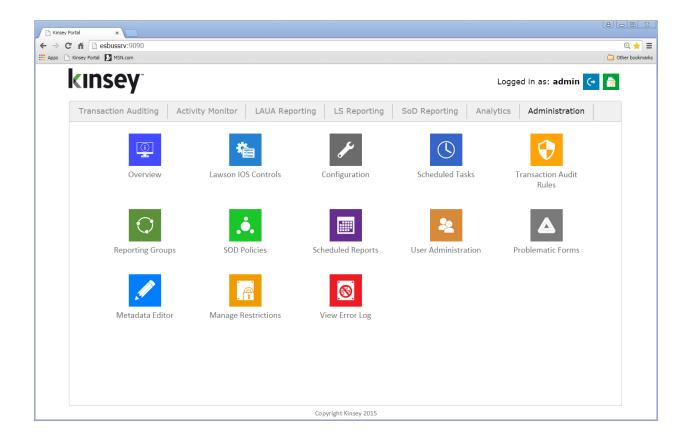
You can set your preferred Home page on the dashboard by selecting the home page icon in the top right corner of your screen. This setting is saved as a browser cookie and will be lost whenever you clear your browser cache.

# **Configuring your LDAP Reporting Profile**

The data used to generate the LS reports is pulled directly from your LDAP database. The LS Dashboard Reports can be executed through your standard browser interface. You can launch the dashboard using the URL provided by your security administrator.

Launch the Security Dashboard from your Windows browser.

Click on the Administration Tab and select Configuration. You will be asked for a user ID and Login. See you security administrator for this information.



Scroll down to the LS Security Configuration option for either Test or Production and click on the + sign.

- LS9 Security Configuration (Production Server)	
LDAP Server: Is3server.corpnet.lawson.com	LDAP User: CN=root,CN=lwsn,DC=ls3server
LDAP Port: 389	LDAP Password: Lawson1975
LDAP Base Search: CN=lwsn,DC=ls3server	LDAP Profile: APS
User LDAP Base Search:	
LDAP Paging Size: 1000	RMID Translation Productline:
LDAP "back-office"	LDAP "Company:Employee" LIVE_EMPLOYEE Service:
Collect Employee 🕑 termination data:	
Employee fields to COMPANY;EMPLOYEE;DATE_HIRED;TERM_D2	

#### Lawson LDAP Server Settings

LDAP Profile: APS

LDAP Profile Enter the default LS Profile you use for reporting. The reporting application will allow you to change the profile prior to running a query but the Profile entered here will be used as the default.

#### **User Active but Terminated Report Requirement**



There is a User security report that will validate if a terminated employee is still active in the security model. The report requires data to be retrieved from the Lawson HR tables. To enable the feature select the 'Collect Employee termination data' check box.

The report will include the field names entered in the Employee Fields to Collect cell. You can collect data for any field that would indicated the employee has been terminated. This would generally be the TERM\_DATA field but a user defined field might also hold the information you need.

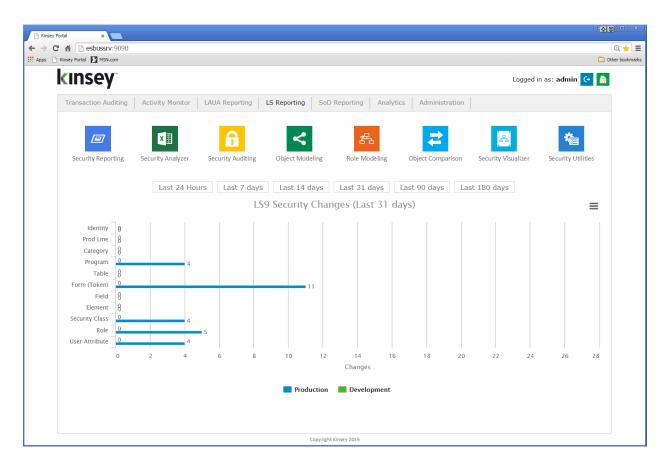
Examples of the fields generally used are: COMPANY, EMPLOYEE, HIRED and TERM\_DATE

# Note: If you do not run the Lawson HR application this report will not work in your environment.

# **Security Admin Reports**

The Security Admin reports are designed specifically for anyone that needs to maintain security functionality in the LDAP model. Although these reports can be used by the auditors, they provide more insight into the technical aspects of the model that is not generally required by an auditor. The Security Analyzer was built specifically for the audit team.

Launch the Security Dashboard and select the Security Reporting icon from the LS Reporting tab.



Start by selecting the server and LDAP profile you want to report on in the top right corner of the screen. You can select to view reports based on current settings or historically snapshots. Historical snapshots can be create through the administration panel.

Production Server	▼ * APS	• H 🗎 🕯	? ↔	
	Da	ata Last Updated: 12/3	3/14 14:43	
				2 <b>0 9</b> 0
Kinsey LS Reporting × ► → C ☆ Besbussrv:9090/KK_LS9Reporti	in - Da - Hall			
Apps 🕒 Kinsey Portal 🚺 MSN.com	IngPortal/			Q, 숫 Dther book
(INSEY <sup>®</sup> Security Reporti	ing		Production Server	APS Hi APS
🖧 Users	중국 Roles	Tasks	Statistics	-∭ Listener
User - All Objects User - Group User - Identities User - Role User - Role - Group User - Role - Task - Form	Role - Task Role - Task - Element Group Role - Task - Form Role - Task - Object Role - Task Counts Role - User Counts Role - Without Tasks	Forms Per Task Tables Per Task Task - All Objects Task - Element Group Task - Form Task - Repeated Forms Task - Repeated Tables	Metadata - Forms   Fields Metadata - Forms   Fields Metadata - Tables Structures Structures - Children Structures - Parents Table Statistics	Form Count Summary User - Form Detail User - Form Summary Users Security versus Activity
User Active - Joan Torminated User Active - no Employee Record User Artiflute Settings User CheckLS is Not Set User CheckLS Setting Users without Roles	Roles Without Users	Task - Table Unassigned Objects Unassigned Tasks		
LS User 'Check LS' Status			gned Objects	
	Not Set	1,200		
19.2%	NO YES	900		1043 997
7.7%	_			
1.176		600		
73	3.1%			
		300		
			1 55 1 0	
		0 Ro	les Tasks System Programs Codes	Tables Forms
		Copyright (c) 2015		

The Security Reporting dashboard comes preconfigured with reports by User, Role, Task (Security Class) and includes statistical information about your model. If you have also purchase the Activity Monitor (Listener) application a separate group of reports will provide you will information on how Lawson is being used.

#### **Report Features**

#### **Pre-Report Filters**

The report filters allow you to restrict the amount of information that will be retrieved from the database prior to generating the report. This is helpful when you are working with a large amount of data any only want a small subsection to analyze.

All of the report filters follow the same convention. The filter options will vary depending on report selected.

Kriney Portal X  Kriney IS Reporting X  Lainson Security 9 Reporting X	
← → C 🛉 🗋 esbussrv:9090/KK_LS9ReportingPortal/filters.htm?SERVERID=LSF_PROD&PROFILE=APS&ID=141	© ☆ 🍰 🗉
🔛 Apps 👔 Knsey ESBus Home Pa 🚺 MSU.com	C Other bookmarks
kinsey Role - Task - Form	□ 🗎 ? 🗘
Server: LSF_PROD   Profile: APS	<u>Hide Search Criteria</u>
Field Selection	
Role All •	
Task All •	
Form All •	
Run Report	

For example, on the Role – Task – Form report you will have the option of filtering by Role, Task (Security Class) or Form. If you need to filter by any other field you can do that once the grid is populated. All filters assume "AND" logic, meaning all values must satisfy the criteria for data to be displayed.

There are 2 methods when using filters. The first simply provides the option of selecting the condition and filling in the value. For example, in the above example to report on a specific Role you would simply change the "Selection" value to "Equals' and fill in the appropriate value. Repeat the process for the Task and Form fields. If you want the application to return all values for a field you do not need to make a selection.

Filter Expressions	
Equals	Value entered must match data exactly.
Contains	Value entered must be contained within the data.
Starts With	Data returned must start with value entered.
Ends With	Data returned must end with the value entered.
Is Between	Date returned must fit within the range selected.

Regular-ExSimilar to OR logic. Entered as value | value | value etc. Useful when<br/>trying to view records with specific dates.

The second method allows you to select from a list of possible values, but can take some time to auto populate depending on the size of your model.

Kinsey Portal X Kinsey LS Reporting X Lawson Secu	rity 9 Reporting ×			<u>0</u>
← → C ↑ Besbussrv:9090/KK_LS9ReportingPortal/filters.ht	tm?SERVERID=LSF_PRO	DD&PROFILE=APS&ID=141		० 🕁 🔬 ≡
Apps 🚦 Kinsey ESBus Home Pa 🚺 MSN.com				Other bookmarks
<b>KINSEY</b> <sup>®</sup> Role - Task - Form			<b>→</b>	<b>ते ?</b> ↔
Server: LSF_PROD   Profile: APS			Hid	e Search Criteria
Field Selection				
Role Advanced •				
Available			Selected	
ACAccountant	A	Select Role		
ACAssetClerk	Add >	< Remove		
ACAssetManager	Auu >	< Remove		
ACDataEntry	Add All >>	<< Remove All		
ACExpert				
AllAccessRole AllAccessRole				
APInquery		Contains •		
ApplicantRole				
APSuper				
ARSuper test description	Add >	< Remove		
AshantiTestRole AshantiTestRole				
BRBiller	*			
Available: 3	/		Selected: 0	
Task All 🔻				
Form All •				
Run Report				
				-

Start by selecting "Advanced" as the condition. The application will display all of the available values associated with the specific field. For instance, in the example above all of the Roles are displayed in the Available column. At this point you have a couple of ways to select the Roles you would like included on the report.

# Adding or Removing Selected Values

While holding down the CTRL key click on the Roles you want added to the report then click on the drop **Add >** button. To remove a values from the list select the items in the 'Selected' column and click on **< Remove**.

🗋 Kinsey Portal 🗙 🌓 Kinsey						_ = X
Kinsey Portal ×      Kinsey     Kinsey     Kinsey     C				CRID 141		
Apps 8 Kinsey ESBus Home Pa MSN.		I?SERVERID=LSF_I	PROD&PROFILE=AP	581D=141		Q, ☆ 🚓 〓
kinsey <sup>*</sup> <sub>R</sub>	ole - Task - Form					▶ 💵 🔒 ? 😋
Server: LSF_PROD   Profile	: APS					<u>Hide Search Criteria</u>
Field Selection						
Role Advanced •						
	Available				Selected	
ACAccountant			Select Role			
ACAssetClerk						
ACAssetManager		Add >		< Remove		
ACDataEntry		Add All >>		<< Remove All		
ACExpert						
AllAccessRole	AllAccessRole					
APInquery			Contains •			
ApplicantRole						
APSuper						
ARSuper	test description	Add >		< Remove		
AshantiTestRole	AshantiTestRole					
BRBiller						
	Available: 37					Selected: 0
Task All 🔻						
Form All •						
Run Report						
Kull Report						

# Adding or Dropping All Values

To add all Roles simply click on the **Add All >>** button. To remove all select the

#### << Remove All button.

Kinsey Portal X Kinsey LS Reporting X Lawson Secur	ity 9 Reporting ×	- <b>D</b> X
← → C ↑ esbussrv:9090/KK_LS9ReportingPortal/filters.ht		ର 🏫 🚍
Apps 8 Kinsey ESBus Home Pa      MSN.com		Ci Other bookmarks
Role - Task - Form		→ III 🚔 ? 💓
Field Selection		
Role Advanced •		
Available		Selected
ACAccountant	Select Role	
ACAssetClerk	Add > < Remove	
ACAssetManager	Add>	
ACDataEntry	Add All >> < Remove All	
ACExpert		
AllAccessRole AllAccessRole		
APInquery	Contains •	
ApplicantRole		
APSuper test description		
AshantiTestRole AshantiTestRole	Add > < Remove	
BRBiller		
Available: 3	7	Selected: 0
Task All		
TASK AII		
Form All 🔹		
Run Report		
		•

#### Adding or Removing Criteria Based Filters

To add Roles based on specific criteria you can use the condition option to make your selection. Start by selecting the condition.

🗋 Kinsey P	ortal X Kinsey LS Reporting X	9 Reporting ×					0 0 X
< → C				ROFTLE=AP	S&ID=141		० ☆ 🍰 ≡
	Kinsey ESBus Home Pa MSN.com						C ther bookmarks
	ISEY Role - Task - Form LSF_PROD   Profile: APS						→ I A C C I C I C I C I C I C I C I C I C
<b>Field</b> Role	Selection Advanced						
	Available					Selected	
	BRExpert		Sele	ect Role		ACAssetManager	
	BRReportingAdministrator	Add >			< Remove	ManagerRole	
	BRRevenue Analyst	Add >			< Remove	POPurchasingManager	
	CustomerRole	Add All	>>		<< Remove All		
	EmployeeRole	1					
	EntryClerk						
	FinancialRole		Cont	tains •			
	FinSup		manager				
	GLAccountant						
	GLReportWritter GLSuper	Add >			< Remove		
	HRClerical						
	Available: 34						Selected: 3
	All • All • Report						

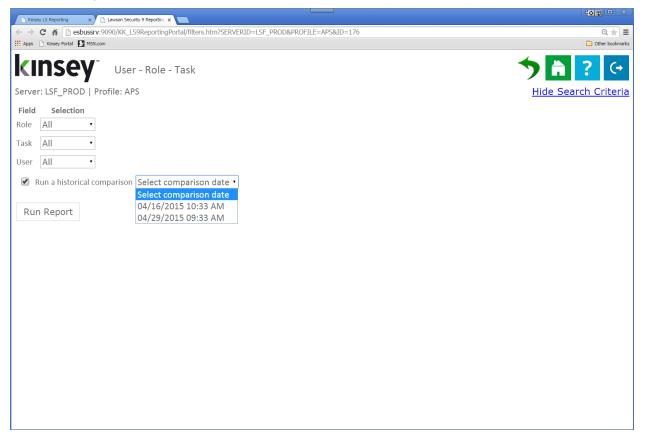
There are 2 options on which you base your logic; Contains and Starts With. In this example I will select "Contains", enter the value of "manager" and select the **Add** > button. As you can see all of the Roles containing "manager" in their ID or name have been moved to the selected list. You can remove items from the Selected list by entering a condition and selecting the **< Remove** button.

Note: In all cases you can Add or Remove by combining the methods or repeating a method as needed. For example you could Add all values starting with "ACCT" and then also Add all values containing "super".

#### **Historical Comparisons**

When you run a historical comparison the application will ONLY return the changes between the current security model and the baseline you are comparing to. This should not be considered a true change audit report but rather a differences report from the last approved security review. You should use the Security Audit Reporting application will reflect the time and date of any security changes and the person who made the change.

After you have selected the appropriate filters check the 'Run a historical comparison' field. The application will prompt you for the time stamped database you would like to compare to. If no comparison dates are available see your system administrator about creating a baseline snapshot.



*Note: You cannot run a historical comparison if you have selected a historical database for reporting. This option will be hidden when running history reports.* 

#### **Changing Pre-Report Filters**

To change your selection criteria without exiting the report simply select the Show Search

Criteria link in the upper right corner of your screen..



#### **Showing and Hiding Columns**

The application has two methods for showing or removing columns from the grid. The first option allows you to set the default columns for all security reports through the LS Security Configuration option on the Administrative Configuration page. Check the fields you would like hidden by default.

	LS9 Security Configuration (Production	on Serve	r)		
awson IOS Controls	LDAP Server:	ls3server.c	orpnet.lawson.com		
onfiguration	LDAP Port:				
cheduled Tasks	LDAP Base Search:	CN=lwsn,E	C=Is3server		
ransaction Audit Rules	User LDAP Base Search:				
Reporting Groups	LDAP Paging Size:	1000			
OD Policies	LDAP "back-office" Service:				
cheduled Reports	Collect Employee termination data:				
Jser Administration	Employee fields to collect:				
Problematic Forms	LS Security Reporting Fields:	Hidden	Friendly Name	Database Field	
/letadata Editor			Attribute	ATTRIBUTE	
/Janage Restrictions			Attribute Value	ATTRIBUTE_VALUE	
/iew Error Log			Audit	AUDITED	
			Available FC	AVAILABLEFC	
			Check LS	CHECK_LS	
			Company	COMPANY	
			Count	ListenerCount	
			Date	DATE	
			Date	ACCESSED_AT_DATE	
			Date/Time	ACCESSED_AT	
			Employee	EMPNUM	
			Field Description	LABEL	
			Form	TOKEN	
			Form Description	TITLE	
			Full Name	FULLNAME	
			Function	FC	
			Hidden	HIDDEN	

#### Note: not all fields show on all reports

The Second option allows you to select the columns at the time you run the report. The application will default to the settings found under the LS Security Configuration option on the Administrative Configuration page.

Expand Groups	Collapse Groups	Clear Filters Show/Hide Columns
Drag a column an	d drop it here to group	by that column
User	▼ Full Name	T-1- T-1.
hroberts	Roberts, Helen	Show/Hide Columns X
hroberts	Roberts, Helen	🕑 User
hroberts	Roberts, Helen	Full Name
hroberts	Roberts, Helen	✓ Role
hroberts	Roberts, Helen	Role Description
hroberts	Roberts, Helen	🗹 Task
hroberts	Roberts, Helen	Task Description
hroberts	Roberts, Helen	✓ Form
hroberts	Roberts, Helen	Form Description
hroberts	Roberts, Helen	Available FC
hroberts	Roberts, Helen	✓ Rule
hroberts	Roberts, Helen	
hroberts	Roberts, Helen	
hroberts	Roberts, Helen	
hroberts	Roberts, Helen	AllAccessRole ACCapitalization

Select the Show/Hide Columns button to select the columns you want displayed.

# **On-The-Fly Report Filters**

You can also filter your results once the grid has been populated. Select the filter icon next to the field name in the header.

← → C ♠ [	esbussrv:9090/KK_LS9ReportingPortal/filters.	htm?SERVERID=LSE_PROD&PROFILE=AP	S&ID=141			Q. ☆
Apps 📄 Kinsey Por						C Other book
kinsey	Role - Task - Form				늇 💼 💵	▶ 🖬 🗎 ? 🤇
erver: LSF_PROD	Profile: APS					Show Search Crite
Expand Groups	Collapse Groups Clear Filters Show/Hide	Columns				5.359 rec
Drag a column and	drop it here to group by that column		$\frown$			
Role	T Role Description T Task	Task Description	T Form	T Form Description	T Available FC	T Rule T
ACAccountant	ACAnalysis	Activity Management Analysist	AC03.6	Equipment Assignment	+,-,A,C,I,N,P	Ψ
ACAccountant	ACAnalysis	Activity Management Analysist	AC34.1	Compute Parameters	A,C,D,I,N,P	Ψ
ACAccountant	ACAnalysis	Activity Management Analysist	AC20.6	Activity Group Budget Header	A,C,D,I,N,P	Ψ
ACAccountant	ACAnalysis	Activity Management Analysist	AC23.1	Spread Codes	A,C,D,I,N,P	Ψ
ACAccountant	ACAnalysis	Activity Management Analysist	AC41.4	Resource Time Entry (AC and GL)	+,-,A,C,D,I,N,P,R	Ψ
ACAccountant	ACAnalysis	Activity Management Analysist	AC07.1	Account Assignment	+,-,A,C,I,N,P	if(form.AGA_ACTIVITY_GRP=
CAccountant	ACAnalysis	Activity Management Analysist	AC20.9	Budget Header Selection	1	Y .
ACAccountant	ACAnalysis	Activity Management Analysist	AC36.1	Activity Total Range	A,C,D,I,N,P	Ψ
ACAccountant	ACAnalysis	Activity Management Analysist	AC18.3	Assigned Vendor Resource Rates	+,-,A,C,D,I,N,P	Υ
ACAccountant	ACAnalysis	Activity Management Analysist	AC37.2	Allocation Group by Step	+,-,A,C,D,I,N,P,R,U	Ψ
ACAccountant	ACAnalysis	Activity Management Analysist	AC10.4	Location	A,C,D,I,N,P	'NO_ACCESS'
ACAccountant	ACAnalysis	Activity Management Analysist	AC20.8	Budget Lock	C,I,N,P	Ψ
ACAccountant	ACAnalysis	Activity Management Analysist	AC37.1	Allocation Group	+,-,A,C,D,I,N,P,R,U	γ
ACAccountant	ACAnalysis	Activity Management Analysist	AC08.1	Category Structure	+,-,A,C,I,N,P,X	Ψ
ACAccountant	ACAnalysis	Activity Management Analysist	AC40.2	Additional Information	C,I	γ
ACAccountant	ACAnalysis	Activity Management Analysist	AC03.5	Asset Assignment	+,-,A,C,I,N,P	'l'
ACAccountant	ACAnalysis	Activity Management Analysist	AC10.1	Activity	A,C,D,I,N,P	'NO_ACCESS'
ACAccountant	ACAnalysis	Activity Management Analysist	AC18.1	Assigned Person Resource Rates	+,-,A,C,D,I,N,P	η.
ACAccountant	ACAnalysis	Activity Management Analysist	AC41.3	AC only Totals	I,N,P	Ψ
ACAccountant	ACAnalysis	Activity Management Analysist	AC10.2	Location Assignment	A,C,D,I,N,P	'NO_ACCESS'
ACAccountant	ACAnalysis	Activity Management Analysist	AC40.1	Journal Entry (AC only)	+,-,A,C,D,I,N,P,R	Ψ
ACAccountant	ACAnalysis	Activity Management Analysist	AC41.2	Additional Information	C,I	η.
ACAccountant	ACAnalysis	Activity Management Analysist	AC32.3	Account Category Selection	I	T
ACAccountant	ACAnalysis	Activity Management Analysist	AC20.4	Activity Budgets by Activity	+,-,C,I,L,N,P	Т
ACAccountant	ACAnalysis	Activity Management Analysist	AC36.2	Activity Total Range Header	D,I,N,P	T
ACAccountant	ACAnalysis	Activity Management Analysist	AC03.3	HR Employee Assignment	+,-,A,C,I,N,P	η.
ACAccountant	ACAnalysis	Activity Management Analysist	AC00.2 Copyright (c) 2015	Calendar	A,C,D,I,N,P	var zz=new mkUsrDateObj(us

🛃 Sort Ascending
🛃 Sort Descending
<b>2</b> × Remove Sort
Group By this column
Remove from groups
Show rows where:
contains
And 🔻
And  contains

Each column as has the option to add on-the-fly filters. When you select the filter icon next to the column header you will see the option "Show rows where:". To add a filter simply select the condition and enter the value. The conditions include; contains, empty, not empty, contains (match case), does not contain, does not contain (match case), ends with, ends with (match case), equals, equals (match case), null, not null. You can nest up to 2 conditions using either AND or OR logic. To change to OR login select the down arrow next the word 'And' and change the option to 'OR'.

#### Grouping

#### **Creating a Group**

The grouping option provides a dynamic way of viewing your data in a summarized format without having to generate a new query. This option can turn a single query into multiple dimensions.

Let's take a look at the following query for Role - Task - Form.

< → C # [	esbussrv:9090/KK LS9ReportingPortal/filters.ht	m2SERVERID=LSE_PROD&PROFILE=AP	S&ID=141			Q &
Apps 📄 Kinsey Po			5040 111			C Other bookma
<b>(Insey</b>	Role - Task - Form				🕥 🚔 💷	, 님 🚔 ? 🤆
erver: LSF PROD	Profile: APS					Show Search Crite
Expand Groups	Collapse Groups Clear Filters Show/Hide C	alumna				
		ournins				5,359 reco
	d drop it here to group by that column					
Role	T Role Description Task	Task Description	T Form	T Form Description	T Available FC	T Rule T
ACAccountant	ACAnalysis	Activity Management Analysist	AC03.6	Equipment Assignment	+,-,A,C,I,N,P	T
ACAccountant	ACAnalysis	Activity Management Analysist	AC34.1	Compute Parameters	A,C,D,I,N,P	T
ACAccountant	ACAnalysis	Activity Management Analysist	AC20.6	Activity Group Budget Header	A,C,D,I,N,P	T
ACAccountant	ACAnalysis	Activity Management Analysist	AC23.1	Spread Codes	A,C,D,I,N,P	Т
ACAccountant	ACAnalysis	Activity Management Analysist	AC41.4	Resource Time Entry (AC and GL)	+,-,A,C,D,I,N,P,R	Υ.
ACAccountant	ACAnalysis	Activity Management Analysist	AC07.1	Account Assignment	+,-,A,C,I,N,P	if(form.AGA_ACTIVITY_GRP=
CAccountant	ACAnalysis	Activity Management Analysist	AC20.9	Budget Header Selection	1	Т
ACAccountant	ACAnalysis	Activity Management Analysist	AC36.1	Activity Total Range	A,C,D,I,N,P	Υ
ACAccountant	ACAnalysis	Activity Management Analysist	AC18.3	Assigned Vendor Resource Rates	+,-,A,C,D,I,N,P	T
ACAccountant	ACAnalysis	Activity Management Analysist	AC37.2	Allocation Group by Step	+,-,A,C,D,I,N,P,R,U	Т
ACAccountant	ACAnalysis	Activity Management Analysist	AC10.4	Location	A,C,D,I,N,P	'NO_ACCESS'
ACAccountant	ACAnalysis	Activity Management Analysist	AC20.8	Budget Lock	C,I,N,P	T
ACAccountant	ACAnalysis	Activity Management Analysist	AC37.1	Allocation Group	+,-,A,C,D,I,N,P,R,U	Υ
ACAccountant	ACAnalysis	Activity Management Analysist	AC08.1	Category Structure	+,-,A,C,I,N,P,X	T.
ACAccountant	ACAnalysis	Activity Management Analysist	AC40.2	Additional Information	C,I	T
ACAccountant	ACAnalysis	Activity Management Analysist	AC03.5	Asset Assignment	+,-,A,C,I,N,P	T.
ACAccountant	ACAnalysis	Activity Management Analysist	AC10.1	Activity	A,C,D,I,N,P	'NO_ACCESS'
ACAccountant	ACAnalysis	Activity Management Analysist	AC18.1	Assigned Person Resource Rates	+,-,A,C,D,I,N,P	T
ACAccountant	ACAnalysis	Activity Management Analysist	AC41.3	AC only Totals	I,N,P	T
ACAccountant	ACAnalysis	Activity Management Analysist	AC10.2	Location Assignment	A,C,D,I,N,P	'NO_ACCESS'
ACAccountant	ACAnalysis	Activity Management Analysist	AC40.1	Journal Entry (AC only)	+,-,A,C,D,I,N,P,R	Υ.
CAccountant	ACAnalysis	Activity Management Analysist	AC41.2	Additional Information	C,I	Υ
CAccountant	ACAnalysis	Activity Management Analysist	AC32.3	Account Category Selection	I. I.	Т
CAccountant	ACAnalysis	Activity Management Analysist	AC20.4	Activity Budgets by Activity	+,-,C,I,L,N,P	Т
CAccountant	ACAnalysis	Activity Management Analysist	AC36.2	Activity Total Range Header	D,I,N,P	Т
CAccountant	ACAnalysis	Activity Management Analysist	AC03.3	HR Employee Assignment	+,-,A,C,I,N,P	T
ACAccountant	ACAnalysis	Activity Management Analysist	AC00.2 Copyright (c) 2015	Calendar	4,C,D,I,N,P	var zz=new mkUsrDateObj(us

By default the query is going to be displayed in detail by Role, Class and Form. But let's say we want to rearrange the list and group it by Form to see all of the Tasks and Roles assigned to each Form.

Start by dragging the 'Form' column header to the open area on the title bar. The header will display with a green check mark once it's in the proper position.

Drag a column and drop it	here to group by that column	•				
Role T	Role De 🍸 Task	Task Description	Form T	Form Description	▼ Rule	<b>T</b>

Alternatively you can select the drop down arrow next to the column title and choose Group by this column.



The grid will be redisplayed and grouped by Form.

Exp	oand Groups	Collapse Grou	ups Clear Filt	ers				5,356 records
For	m 🔺 🗙							
	Role	Ÿ	Role Descriptio	n ⊤ T	Task T	Task Description	▼ ▲ ▼ Form Description	🝸 RL 🖛 📥
►	Form: HR1	10.4 (4)						
►	Form: HR1	11.1 (8)						
►	Form: HR1	11.2 (6)						
►	Form: HR1	11.3 (1)						
►	Form: HR1	12.1 (4)						
►	Form: HR1	13.1 (6)						
►	Form: HR1	13.2 (6)						
►	Form: HR1	13.3 (6)						
►	Form: HR1	13.4 (6)						
►	Form: HR1	14.1 (4)						
►	Form: HR1	15.1 (4)						

You can now see the number of assignments for any specific Form. To see those assignments click on the arrow left of the Form name.

Exp	and Groups Collapse	Groups Clear Filters				5	,356 recc
Forr	n 🔺 🗙						
	Role	T Role Description	▼ Task	Task Description	T 🗅 T	Form Description	T RU T
•	Form: HR10.4 (4)						
►	Form: HR11.1 (8)						
►	Form: HR11.2 (6)						
►	Form: HR11.3 (1)						
-	Form: HR12.1 (4)						
	HRClerical		HRSetup	All Access to HR Setup form	s H	Employee Securit	y 'A
	HRDirector		HRSetup	All Access to HR Setup forms	HR	Employee Security	'AL
	HRClerical		HRSetupInq	Inquiry only access to HR S.	H	Employee Securit	y 'A
	HRGeneralist		HRSetup	All Access to HR Setup forms	HR	Employee Security	'AL
•	Form: HR13.1 (6)						

The grid now displays the Roles, Tasks and Rule associated with the Form.

#### Grouping - Nested

Grouping can be done using multiple fields. See 'Grouping' to add your first group. Once this is complete you can add a second level by simply dragging another header to the title bar. In this example we will add Task to the Group.

orm <b>△ × </b> Task ×					5,356 recor
Role	Role Description	⊤ Task	Task Description	▼ △ ▼ Form Description	⊤ Rul ⊤ 4
Form: HR10.2 (2	)				
Form: HR10.3 (2	)				_
Form: HR10.4 (2	)				
Form: HR11.1 (5	)				
Form: HR11.2 (4	)				
Form: HR11.3 (1	)				
Form: HR12.1 (2	)				
► Task: HRSet	up (3)				
► Task: HRSet	upInq (1)				
Form: HR13.1 (3	)				

As you can see the system will now report on the number of Tasks the Form can be found in and the number of Roles assigned to the Task. You can view the Roles assigned by expanding the list using the arrow left of Task.

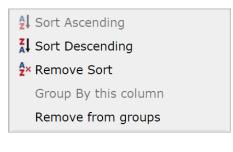
#### Grouping – Expand, Collapse or Remove

At the top of each report are additional options you can use when Grouping is performed.

Expand Groups	Collapse Groups
Form A ×	Task 🗙

Simply select the Expand or Collapse buttons to display or hide the grouping details. To remove a group entirly select the 'x' next to the title on in the header.

Alternatively you can select the filter icon next to the column title and choose Remove from Groups.



#### **Grouping – Remove Filters**

Any filter added to a column is maintained when Groups are used. To remove column filters select the Remove Filters button. The Groups will be maintained but the column filters will be removed.

*Note: This does not affect the 'pre-report' filters created prior to generating the query.* 

#### Sorting

#### Adding a Sort Option

There are a couple of ways to sort the rows once the grip is displayed. The simplest method is to just click on the column Title.

Drag a column and	d drop it	here to group by that	colum	n		-		•
Role	Ÿ	Role Description	T	Task	T	Task Description	Form 🔺 T	Form Description
HRGeneralist				HRSetup		All Access to HR Setup f	HR00.1	Company
HRClerical				HRSetup		All Access to HR Setup f	HR00.1	Company
HRClerical				HRSetupInq		Inquiry only access to H	HR00.1	Company
HRDirector				HRSetup		All Access to HR Setup f	HR00.1	Company
HRClerical				HRSetupInq		Inquiry only access to H	HR00.2	Canada Payroll Account
HRDirector				HRSetup		All Access to HR Setup f	HR00.2	Canada Payroll Account
HRGeneralist				HRSetup		All Access to HR Setup f	HR00.2	Canada Payroll Account
HRClerical				HRSetup		All Access to HR Setup f	HR00.2	Canada Payroll Account

You can also select the arrow next to the column header and choose to sort in Ascending or Descending sequence.



#### **Removing the Sort Option**

Select the filter button next to the column header and choose 'Remove Sort'



#### Saving Security Reports

You can save a report by selecting the save icon once the report has been displayed on the screen. The application saves the search criteria and not the results of the query. Each time you run the report the application will use the saved filters to generate a new report.

Note: Saving a report does not save the sort sequence, grouping, column filters or historical flag that may have been used prior to saving the report.

H Save Repo	ort	×
Report Name: Report Description	pn:	
	Save Report	

#### **Running Saved Report**

All saved reports are displayed as a row on the saved reports query. From the Security Reporting Home Page select the Save icon at the top of the screen. A list of saved reports will be displayed. Click on the Report Name to Run, Schedule or Delete the report.

Note: If a user is blocked from running specific types of reports (i.e. Roles) in the security section of User Administration they will not be able to run saved reports of the secured type.

#### **Exporting and Printing**

You can export or print your final query to Microsoft Excel, PDF of HTML once you have set all of your parameters by clicking on the appropriate icon at the top of the page.



The MS Excel export will maintain the grouping, sorting, columns and filters you have created in the query, but the column widths will need to be adjusted once you are in Excel.

Is the example below the query was grouped by Role prior to the export. To view the Role detail form within Excel click on the `+ sign next to the Role.

	A321	7 <del>-</del> (a	∫∗ ADMIN					
2		A Role	B Role Description	C Security Class	D Class Description	E	F	G
		ADMIN	ADMIN	ActivityManagem1	[AC] System Code Tokens.Categories.Programs	ACVW.1	Build GL Accounting Unit View	'ALL ACCESS'
	653	HRPOWER	HRPOWER	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL ACCESS'
	979	TESTADMIN	TESTADMIN	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL ACCESS'
	1305	BENUSER	BENUSER	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL ACCESS'
	1631	PAYUSER	PAYUSER	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'
	1957	ACCT-SUPV	ACCT-SUPV	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'
e.	2283	AMEN	AMEN	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'
E.	2609	PA	PA	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'
E.	2935	PAYROLL	PAYROLL	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'
Ð	3261	HR	HR	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'
E	3587	HRUSER	HRUSER	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'
E.	3913	ACCT-CB	ACCT-CB	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'
E.	4239	WEB	WEB	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'
E.	4565	TECHNICAL	TECHNICAL	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'
	4891	TREASURY	TREASURY	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'
E	5217	AP	AP	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'
E.	5543	AP-ADMIN	AP-ADMIN	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'
	5869	URC	URC	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'
E	6195	MGMTINQ	MGMTINQ	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'
	6521	MikesClass	This also is a test	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'
	6847	PA-FIN-	PA-FIN-	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'
	7173	POWERUSER	POWERUSER	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'
	7499	ACCT	ACCT	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'
	7823	TRAINING	TRAINING	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'
	7824							

#### Drilling

The drill feature allows you to move up or down the security tree to view settings for either Roles or Tasks. The following drill assignments are available.

- Drill from a Role down to see the assigned Tasks
- Drill from a Role up to see the assigned Users.
- Drill from a Task down to see the assigned Forms.
- Drill from a Task down to see all of the assigned Objects.
- Drill from a Task up to see the assigned Roles.

To execute a drill select on the linked object you need to review. In the example below I clicked on the **<u>HRGeneralist</u>** Role and was provided the option of viewing the Tasks assigned to HRGeneralist or the Users that have been assigned the HRGeneralist Role.

Drag a colu	imn and drop it l	nere to gro	up by that colum	in				
Role	T	Role Desc	ription T	Task T	Task Description	Form 🔺 🝸	Form Description 🛛 🔻 🕶	Rul 🝸
HRGene	RGeneralist			HRSetup	All Access to HR Setup f	HR00.1	Company	'AL
HPClari	Role   Task			HRSetup	All Access to HR Setup f	HR00.1	Company	'AL
HRCleri	User   Role			HRSetupInq	Inquiry only access to H	HR00.1	Company	'I,N
HRDirector				HRSetup	All Access to HR Setup f	HR00.1	Company	'AL
HRClerical				HRSetupInq	Inquiry only access to H	HR00.2	Canada Payroll Account	'I,N
HRDirector				HRSetup	All Access to HR Setup f	HR00.2	Canada Payroll Account	'AL
HRGenerali	ist			HRSetup	All Access to HR Setup f	HR00.2	Canada Payroll Account	'AL
HRClerical				HRSetup	All Access to HR Setup f	HR00.2	Canada Payroll Account	'AL

By selecting **Role|Task** a new browser page will open displaying all of the Tasks assigned to this Role.

Drag a column and drop it here to group by that column									
Role 1	Role Description	Ÿ	Task	Task Description	Ţ				
HRGeneralist			DataAreaAccess						
HRGeneralist			HRFiles	HR Files					
HRGeneralist			HRReports	All Access to HR Reports					
HRGeneralist			HRSetup	All Access to HR Setup forms					
HRGeneralist			HRUpdatePrograms	All Access to HR Update Programs					
HRGeneralist			IFSubsystem	IF Subsystem					
HRGeneralist			PAFiles	PA Files					
HRGeneralist			PAReports	All Access to PA Reports					
HRGeneralist			PASetup	All Access to PA Setup forms					
HRGeneralist			PRFiles	PR Files					
HRGeneralist			PRReports	All Access to PR Reports					
HRGeneralist			PRUpdatePrograms	PR Update Programs					

You can then drill on a specific Task to see the Forms and their rules assigned to the Task.

Drag a column and drop it here to group by that column											
Task	Task Description	T Form T	Form Description	⊤ Rule ⊤ 4							
HRSetup	All Access to HR Setup forms	HR30.2	Base Currency	'ALL_ACC							
HRSetup	All Access to HR Setup forms	HR86.6	Test Source	'ALL_ACC							
HRSetup	All Access to HR Setup forms	HR65.1	Human Resource Writer Title Creation	'ALL_ACC							
HRSetup	All Access to HR Setup forms	HR88.4	Human Resource Codes - Disability	'ALL_ACC							
HRSetup	All Access to HR Setup forms	HR86.8	Test User Field 3	'ALL_ACC							
HRSetup	All Access to HR Setup forms	HR18.3	State Reporting Information - Wyoming	'ALL_ACC							
HRSetup	All Access to HR Setup forms	HR65.7	Human Resource Writer Detail Selection	'ALL_ACC							
HRSetup	All Access to HR Setup forms	HR81.4	Competency	'ALL_ACC							

Alternatively you can also drill up the security tree. If you start with the Task - Form query you can drill up to the Roles assigned to a Task and continue to drill up to the Users assigned to a Role.

For example let's look at the Role – Task query. By drilling on the Role **ACAssetManager** I have the option of drilling up to the Users assigned to this Role.

Drag a column and drop i	t here to group by that	column					
Role 🔺	T Role Description	Ϋ	Task T	Task Description	T A		
ACAssetClerk			ACAnalysis	Activity Management Analysist			
ACAssetClerk			AMProcessing	Asset Management Processing			
ACAssetClerk			DataAreaAccess				
ACAssetClerk			PRFiles	PR Files			
ACAssetManager			ACCapitalization	Activity Capitalization 1			
ACAssetManage	etManager		DataAreaAccess				
ACBRJobSchedul User   Role			ACBRJobScheduler	AC and Br Job Scheduler Jobs			
ACBRJobSchedul			DataAreaAccess				

The User - Role query will automatically be displayed listing the User assigned.

Drag a columr	Drag a column and drop it here to group by that column										
User T	Full Name	▼ Role	T Role Description	Ϋ							
lawson	Lawson, Lawson	ACAssetManager									
mnitka	Nitka, Mike	ACAssetManager									

#### **Reports List**

#### Users

User – All Objects User – Group User – Identities User – Role User – Role – Group User – Role – Task (Security Class) User – Role – Class – Form User Active – but Terminated Requires Lawson HR for validation User Active – no Employee Record Requires Lawson HR for validation User Attribute Settings User CheckLS is Not Set User CheckLS Setting

*Note: Refer to the LS Security Configuration for more information configuring the User Active but Terminated query* 

#### Roles

Users without Roles

Role – Task (Security Class) Role – Task – All Objects Role – Task – Element Group Role – Task – Form Role – Task Counts Role – User Counts Roles Without Tasks Roles Without Users

#### Tasks (Security Classes)

Forms Per Task Tables Per Task Task – All Objects Task – Element Group Task – Form Task - Repeated Forms Task - Repeated Tables

Task – Table

Unassigned Objects

Unassigned Classes

# **Ancillary Data**

- Metadata Forms
- Metadata Forms-FC Description
- Metadata Forms|Fields
- Metadata Tables

Structures

- Structures Children
- Structures Parents

Table Statistics

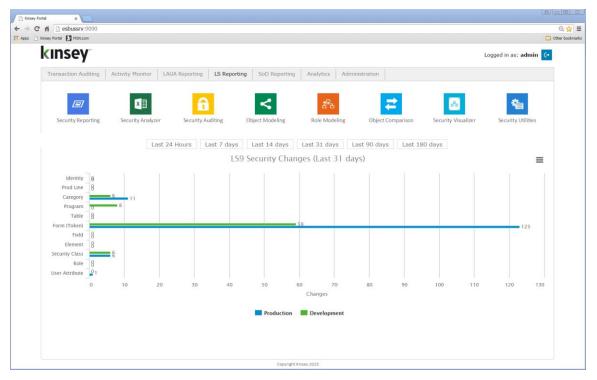
# Listener

Form Count Summary User Class Form Summary User Form Detail User Security versus Activity

#### **Security Analyzer**

The Security Analyzer is designed specifically for anyone that needs to audit security functionality in the LDAP model. Although these reports can be used by the security administrator, they can only be run at the user level. Reports on how Roles and Task (Security Classes) are defined are part of the security administrator reports.

Launch the Security Dashboard and select the Security Analyzer icon from the LS Reporting tab.



#### Selecting a Server

Start by selecting the server containing your LDAP data. The system may be setup to report on your test, development and production systems. The system will automatically retrieve a list of valid Roles, Users and System Codes (Categories) to choose from.

	sbussrv:9090/LS9_Report/				@ ☆] ≡
Apps 🚷 Kinsey ESBus H	Iome Pa MSN.com				Cther bookmarks
kinsey <sup>*</sup>	Security Analyzer				🚔 ? 😋
	Lawson Server Selection Select Server http://is/Server.corpnet.lawson.com http://is/Server.corpnet.lawson.com	Roles (with tasks attached)	Users (with roles attached)	System Codes	

#### **Refreshing Your Data**

To reduce the impact on your LDAP server the Security Analyzer does not pull data from LDAP in real time unless you select the Refresh Security link in the top right corner of your browser page. The refresh option rebuilds the Analyzer tables prior to generating a report. This will provide real-time security settings.

Refresh Security Data last updated: Thu Jan 08 14:37:24 CST 2015

#### **Creating a New Report**

To create a new report select the New Report icon in the top right corner of your browser page.



The page will then allow you to select the Roles, Users and System Codes you would like displayed on the report. Then simply enter a report name and optional report description and save your report.

*Note: All "Self-Service" users can be restricted from this report through the Administration page by your Kinsey software administrator.* 

#### Running an Saved Report

Once a server has been selected the page will display all previously save reports. To run saved reports simply click on the report name. Keep in mind that the *Report Options* are not saved with the reports selection criteria. You may want to review the report options prior to running the report. The report will be generated in Microsoft Excel and may appear at the bottom of your browser page depending on the browser being used.

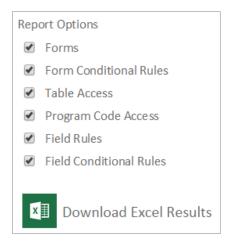
	🗋 Kinsey Security Analyzer 🛛 🔪		
← → C fi  esbussrv:9090/LS9_Report/			ର 🕁 ≡
Apps 🚯 Kinsey ESBus Home Pa 🚺 MSN.com			C Other bookmarks
KINSEY <sup>*</sup> Security Anal	yzer		📔 🔒 ? 😋
Lawson Server Selection http://Is3server.corpnet.lawson. •			Refresh Security Data last updated: Thu Jan 08 14:37:24 CST 2015
Saved Reports	Roles (with tasks attached)	<ul> <li>Users (with roles attached)</li> </ul>	✓ System Codes
All 2 3 AM & HR 2 1 5 AM & HR - Just FNELSON 2 3 Financial Users 2 3 GL45 Access 2 3 Only Roles 2 3 Sara Miller 2 5 Report Options 2 Forms	<ul> <li>ACAssetManager</li> <li>ACDataEntry</li> <li>APSuper</li> <li>ARSuper</li> <li>AllAccessRole</li> <li>FinSup</li> <li>GLAccountant</li> <li>HRDirector</li> <li>PortalBookmarkAdminRole</li> </ul>	<ul> <li>fnelson (Nelson, Frank)</li> <li>hroberts (Roberts, Helen)</li> <li>hrogers (Rogers, Hal)</li> <li>lawson (Lawson Lawson)</li> <li>Isadm (Lawson Admin)</li> <li>Isuser (Lawson User)</li> <li>mnitka (Nitka, Mike)</li> <li>pfadmin (PFADMIN PFADMIN)</li> <li>smiller (Miller, Sarah)</li> </ul>	<ul> <li>AC - Activity Management</li> <li>AD - Avg Daily Balance</li> <li>AM - Asset Management</li> <li>AP - Accounts Payable</li> <li>AE - Accounts Receivable</li> <li>BL - Billing</li> <li>BN - Benefits</li> <li>BR - AC Billing Revenue</li> <li>CB - Cash Ledger</li> <li>CW - Contract Work</li> <li>CX - Case Carts</li> <li>DT - Bills of Exchange</li> <li>EB - Budget Architect</li> <li>ED - EDI</li> <li>EE - Employee Expense</li> </ul>
<ul> <li>Form Conditional Rules</li> </ul>			EN - Enterprise Reporting
✓ Table Access	Report Name		
Program Code Access	Query Description		
<ul> <li>Field Rules</li> </ul>			
<ul> <li>Field Conditional Rules</li> </ul>			A
	SAVE CANCEL		



Select your preferred MS Excel format.

Once the generation process is complete you will see an option to download the Excel document in the lower left corner of the selection screen under the Report Options section.

*Note:* You can filter out specific user identities to prevent users from displaying on this report. This is generally used to filter our Self Service users



#### Editing a Saved Report

To edit a saved report select the pencil icon next to the report name, make the appropriate changes and save the report.

#### **Deleting a Saved Report**

To delete a saved report select the delete icon next to the report name and confirm the delete message.

The page at esbussrv:9090 says:						
Are you sure that you want to de Miller"?	elete selection name	ed: "Sara				
	ок	Cancel				

#### **Report Options**

Depending on what you need to review the report will include security setting for Forms, Form Conditions, Tables, Program Codes, Fields and Field Conditions. You can select the report option in the lower left section of your browser page.

*Note: These options are not saved when you create or edit a report and will always be checked by default.* 

#### **Reading the Analyzer Report**

The security report is fairly intuitive, but there are some features that warrant an explanation.

#### **Users Assigned Roles**

	19	0- 0	○ 保 Q 零 (A):					380363195.xisx - Micr	osoft Excel					-
1	Home	Insert	Page Layout Formulas	Data Revie	ew View	Developer Add-Ins								19 -
X	Cut		Calibri - 10 - A	. = = -		Wrap Text Gener	al •	Normal	Bad Good	Neutral	Calculation	Σ AutoSum · A	8	
10	Copy		B Z U A		-	Merge & Center - S -	% , 18 28 Conditions	I Format Check Coll	Explanatory Input	Unked Cell	Note Insert Delete	Fill - Sort &	Find &	
		at Painter					Formatting	* as Table *		Chinese cent		- 📿 Clear * Filter	- Select -	
	board	- P.	Font	- E-1	Alignment	6	Number 9		Styles		Celli	Editing		
Ľ	152		f NO ACCESS											
	Α	В	c	D	E	F	G	н	1	J	к	la construction de la construcción de la construcci	M	
1	Summ	ary of Law	son Access (LS9 Security) - Forms				ACAssetClerk				Roles assigned to User			
2	(no de	scription)					WHCLGOOMINE ProcessFlowlast Accessflowlast Accessflowlast Accessflowlast Accessflowlast Accessflowlast Accessflowlast Accessflowlast Accessflowlast Accessflowlast Accessflowlast Accessflowlast Accessflowlast Accessflowlast Bioleccia Biochola Bioc	PortalBookmarkAdminRole BatchRole	SuperÁdminitole	ACAssetClerk SODGLADUpdate ACDataEntry TiscLevel05 ACDepert Super Annumbale Annumbale AllAccessible ASuper	ProcessFlowRole	FormPersonalizationRole PortalisationRole processFlowInde ProcessFlowInde SuperAdminiBole BacchRole LawsonQueryToolsRole AllAccessRole	ACAssetManager GLACCT48 GLACCT5G APlinquery APluger GLACcountant	
3											Users			
	Sys	Form ID	Title	Role	Security Class	Available Functions	smiller	Isuser	Isadm	mnitka	pfadmin	broberts	fnelson	
5			Activity Group	- ANNE	secondy class	A,C,D,I,N,P	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS	NO ACCESS	NO ACCESS	NO ACCESS	
10			Calendar			A.C.D.I.N.P	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL ACCESS	NO ACCESS	NO ACCESS	NO ACCESS	
15			Activity Group Purge Status			CUNP	ALL ACCESS	NO ACCESS	NO ACCESS	ALL ACCESS	NO ACCESS	NO ACCESS	NO ACCESS	
18			Mass Activity Copy			+,-,A,C,D,F,I,M,N,P,R,U,V,Z		NO ACCESS	NO ACCESS	ALL_ACCESS	NO ACCESS	NO ACCESS	NO ACCESS	
20			Additional Parameters			NO FC	ALL ACCESS	NO ACCESS	NO ACCESS	ALL ACCESS	NO ACCESS	NO ACCESS	NO ACCESS	
	m		Inquire Filter			NO FC	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS	NO ACCESS	NO ACCESS	NO ACCESS	
22	4.0	AC01.3												

The user ID will be display on row 4 next to the column header. The Roles assigned to each user will appear in column directly above the user ID (shown in yellow above).

#### **Assigned Forms**

The security rule displayed for each user/form reflects the **least restrictive** access to that form for the user. This is very import considering the any form could be in multiple security class (tasks).

<b>C.</b>		<b>17</b> - (1	- 🗋 🖆	; 🖨 🛕 🖤 😰 🔹				380363195.xl	sx - Microsoft Excel		
<b>C</b>	н	ome	Insert	Page Layout Formulas Data	Review Vie	w Developer	Add-Ins				
Norr		out Pr	e Break O	stom Full Itews Screen Screen Show/Hide	9	om 100% Zoom to Selection	New Arrange Freeze Window All Panes	Split         D View Side by Side           Hide         Lat Synchronous Scrolling           Unhide         Lat Reset Window Position           Window         Window	Save Switch Macros		
_		48	DOOK VIEWS			200m		window	Macros		
1 2		48 A	B	J* NO ACCESS	D	F	r	G	н	1	
1 2		A Sys	в	L	U	E	r	6	н		J
	4		Form ID	Title	Role	Security Class	Available Functions	smiller	Isuser	Isadm	mnitka
	5	AC	AC00.1	Activity Group			A,C,D,I,N,P	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS
	10	AC	AC00.2	Calendar			A,C,D,I,N,P	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS
	15	AC	AC00.3	Activity Group Purge Status			C,I,N,P	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS
	18	AC	AC01.1	Mass Activity Copy			+,-,A,C,D,F,I,M,N,P,R,U,V,	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS
J	20	AC	AC01.2	Additional Parameters			NO FC	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS
	22	AC	AC01.3	Inquire Filter			NO FC	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS
1	24	AC	AC01.4	Automatic Activity			A,C,D,I	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS
	26	AC	AC01.5	Automatic Level			A,C,D,I	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS
	28	AC	AC02.1	Status			+,-,A,C,I	A	NO ACCESS	NO ACCESS	A,I
		AC	AC03.1	Resource			A,C,D,I,N,P	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS
	36	AC	AC03.2	AC Person Assignment			+,-,A,C,I,N,P	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS
	40	AC	AC03.3	HR Employee Assignment				ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS
1		AC	AC03.4	Vendor Assignment			+,-,A,C,I,N,P	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS
	48	AC		Asset Assignment				ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS
		AC		Equipment Assignment				ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS
	56	AC	AC03.7	Role Assignment			+,-,A,C,D,I,N,P	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS

The report will also display the available function codes for each form as a basis of understanding exactly what functions are available when ALL\_ACCESS is display. If a user has less than full access the exact function codes will be displayed.

Each cell can have one of 4 values:

- ALL\_ACCESS
- NO ACCESS
- Function codes allowed
- COND\_RULE

When COND\_RULE is displayed you will need to reference the Form Conditions sheet for more information.

#### Assigned Roles and Security Classes

To see the Roles and Security Classed (tasks) assigned to the user select the "+" icon next to the desired row.

*Note: by default Excel will align the plus sign below the desired row instead of next to the row. You can change this setting by select the Data tab, clicking on the small arrow in the Outline section and un-checking the Summary rows below detail option.* 

		Settings ? 🗴		
Data Review	w View Developer Add-I	ns		Direction
Connections	2↓ 2 A		Hide Detail	Summary rows below detail     Summary columns to right of detail
🖙 Edit Links	Advanced	Text to Remove Data Consolidate What-If Columns Duplicates Validation - Analysis -	Group Ungroup Subtotal	Automatic styles
Connections	Sort & Filter	Data Tools	Outline	
				<u>Create</u> Apply Styles OK Cancel

In the example below when I expand form AC10.1 I can see that it has been assigned to 4 different security classes and 4 different Roles. The report will show any Role or Security Class associated with the list of user on the report. *This is not necessarily a reflection of all of the Roles and Security Class this form may be found on.* 

1	2	4	A B	С	D	E	F	G	Н	1	J
		S									
	4	C	ode Form I	D Title	Role	Security Class	Available Functions	smiller	lsuser	lsadm	mnitka
-1	93	3 A	C AC10.:	Activity			A,C,D,I,N,P	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS
	94	4 A	C AC10.:	Activity	ACAccountant	ACSetup	A,C,D,I,N,P	ALL_ACCESS			ALL_ACCESS
	95	5 A	C AC10.:	Activity	ACAssetManager	ACCapitalization	A,C,D,I,N,P	ALL_ACCESS			
	96	6 A	C AC10.:	Activity	ACExpert	ACCapitalization	A,C,D,I,N,P	ALL_ACCESS			ALL_ACCESS
	· 97	7 A	C AC10.:	Activity	ACExpert	ACSetup	A,C,D,I,N,P	ALL_ACCESS			ALL_ACCESS
Ш	98	BA	C AC10.:	Activity	FinSup	ACAnalysis	A,C,D,I,N,P				I
L	99	9 A	C AC10.:	Activity	FinSup	ACDataEntry	A,C,D,I,N,P				1

By showing the access for each Role and Security Class you can determine if the user has multiple access points to this form. Keep in mind that the *least restrictive* method is always displayed on the summary line.

#### **Assigned Form Conditions**

To see any form conditions for a user select the Form Conditions worksheet.

8	Home	🕷 🗋 💕 🤀 Insert Page		∓ ormulas Data	n Review Vie	380363195.xlxx - Microsoft Excel
	F22 $\mathbf{r}$ $\mathbf{f}$					
	A	В	С	D	E	F
1	User	SysCode	Form	Role	Security Class	Conditional Logic
2	mnitka	AC	AC07.1	FinSup	ACAnalysis	if{form.AGA_ACTIVITY_GRP=='SRM'}{'ALL_ACCESS';}else{'I,N,P';}
3	smiller	HR	HR11.1	ManagerRo ESS		if(isElementGrpAccessible('COMP_EMPLOYEE','I','HR',form.EMP_COMPANY,form.EMP_EMPLOYEE)}('ALL_ACCESS';}else{'NO_ACCESS';}
4						
5						

# Assigned Tables

To see a user's table access select the Tables worksheet. This worksheet is very similar to the Form worksheet only reflects table names instead of form names. See Assigned Form for a more detailed explanation..

#### **Assigned Program Codes**

To see a user's available Program Codes select the Program Codes worksheet. This worksheet is very similar to the Form worksheet only reflects Program Codes instead of form names. See Assigned Form for a more detailed explanation.

#### **Assigned Fields**

To see a user's has special conditions tied to a specific field, select the Fields worksheet. This worksheet is very similar to the Form worksheet only reflects Field names instead of form names. See Assigned Form for a more detailed explanation.

#### Assigned Field Conditions

To review any conditional logic assigned to a Field, select the Field Condition worksheet. This worksheet is very similar to the Form Condition worksheet only displays field names instead of form names.

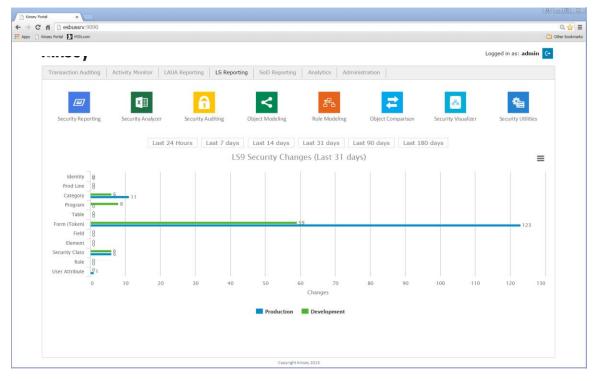
#### **Function Code Legend**

The Function Legend provides a brief description of the purpose of each function code for each form.

# **Change Audit Reporting**

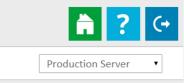
The Change Audit Report builder provides a streamlined approach tracking all changes made to your Lawson Security model. This flexible report writer allows you to track the security changes most important to you and setup automatic email notifications.

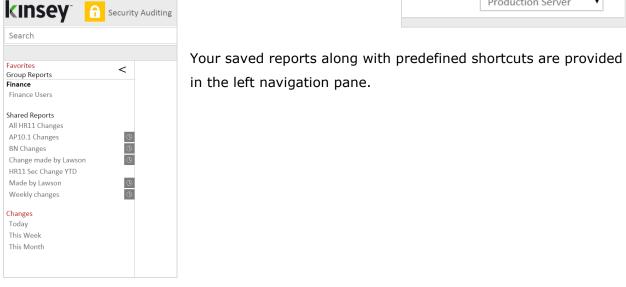
*Note: Lawson Security Auditing must be enabled in the Lawson Security Administrator application before using this application.* 



Launch the Security Dashboard and select the Security Auditing icon from the LS Reporting tab.

Start by selecting the appropriate server in the top right corner of the screen.



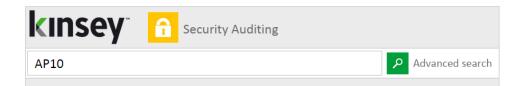


Kinsey Security Auditing ×	
	/?SERVERID=LSF_PROD&QUERY=ap10&_nq=1&_s=1 Q
Apps 🚺 Kinsey ESBus Home Pa 🚺 MSN.com	Cherb
KINSEY 🔂 Securit	Auditing 🕮 📐 🖬 🚘 🔒 ? 🕻
ap10	Advanced search Production Server   Results per page: 25
	Action Date/Time User Affects Profile Role Security Class Type Object Previous Rule Current Rule
Favorites <	🧈 D-Delete 11/23/2014 11:23 PM lawson - DPS - APSetup01a TKN AP10.8 'ALL_ACCESS' - 💶 🌽
Finance Finance Users	🦆 U - Update 11/23/2014 11:23 PM lawson - DPS - APSetup01a TKN AP10.8 'ALL_ACCESS' 'ALL_ACCESS' 💶 📐
Finance Users	🎶 A - Add 🛛 11/23/2014 11:23 PM lawson - DPS - APSetup01a TKN 🗛 P10.6 - 'ALL_ACCESS' 💷 📙
hared Reports All HR11 Changes	🧈 A - Add 11/23/2014 11:23 PM lawson - DPS - APSetup01a TKN AP10.7 - 'ALL_ACCESS' 💷 📐
All HR11 Changes (S)	🧈 A - Add 11/23/2014 11:23 PM lawson - DPS - APSetup01a TKN AP10.4 - 'ALL_ACCESS' 💷 📐
BN Changes	🧈 A - Add 11/23/2014 11:23 PM lawson - DPS - APSetup01a TKN AP10.5 - 'ALL_ACCESS' 💶 🏊
Change made by Lawson (S) HR11 Sec Change YTD	🧈 A - Add 11/23/2014 11:23 PM lawson - DPS - APSetup01a TKN AP10.2 - 'ALL_ACCESS' 💶 📐
Made by Lawson	🎶 A - Add 11/23/2014 11:23 PM lawson - DPS - APSetup01a TKN AP10.3 - 'ALL_ACCESS' 💶 📐
Weekly changes	🏓 A - Add 11/23/2014 11:23 PM lawson - DPS - APSetup01a TKN AP10.1 - 'ALL_ACCESS' 💶 📐
Changes	🏓 A - Add 11/23/2014 11:23 PM lawson - DPS - APSetup01a TKN AP10.8 - 'ALL_ACCESS' 💶 📂
Today This Week	🔑 A - Add 11/23/2014 11:23 PM lawson - DPS - APSetup01a TKN AP10.9 - 'ALL_ACCESS' 🔟 📙
This Month	Previous 1 Next
	Page 1 of 1 pages (0.19 seconds)
	Copyright(c) 2015 - ver 1.2

The audit query will display all results based on the selected criteria. This information comes from Lawson tables created when Security Auditing is activated. If you are not sure if Security is set up to track changes refer to your Lawson Security Admin for more information.

### **Quick Search**

The easiest way to find any change made to a user or form is to enter the information you are searching for in the search bar.



The application can search for Actions, Dates, Users, Role, Security Classes, Object and Rules using the quick search feature.

### **Advanced Search**

For more advance searches where you might want to combine criteria use the Advance Search link next to the search icon.

Column Name:	Search Criteria:	Prompt at runtime:	
Any Field	▼ AP10		
Column Name:	Search Criteria:	Prompt at runtime:	
Audit Date/Time	Beginning of Month      Current Date		
Column Name:	Search Criteria:	Prompt at runtime:	
Not Selected   Not Selected	▼		
Column Name:	Search Criteria:	Prompt at runtime:	
Not Selected   Not Selected	<b>v</b>		
Column Name:	Search Criteria:	Prompt at runtime:	
Not Selected   Not Selected	▼		

In this example I'm searching for all security changes made to fnelson since the beginning of the month.

By setting the default Search Type to "Match All" the application uses "AND" logic to retrieve the data. This simply means that both filter conditions must be true for a record to be displayed. If you want the system to use "OR" logic simply change the Search Type to "Match 1 or More". When this is done then either of the selection filters needs to be true to return data.

Available Column Names are:

- Any Field (searches any field use the criteria entered)
- Audit Date
- User Name (User who made the security change)
- User Affected (the User affected by the change. This only reflect changes made to information containing the User ID)
- Profile
- Role
- Security Class
- Object Type
  - PGM Programs
  - TKN Tokens (forms)
  - CAT Category (system codes)
  - TBL Tables
  - EXE Executable
  - PDL Product Line
  - TYP Type
  - ELG Element Group
  - RPT Report
  - o TFL
  - o RMO
  - o FLD
  - o HDN
  - o DTL
- Object
- Value
- Changed To
- Action

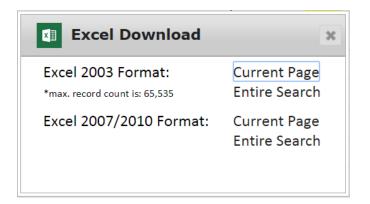
# Prompt at Runtime

This option allows you to flag the criteria you will allow a user change when a report is run from the saved report navigation pane. For example you may set up a report to check for any HR11.1 changes within a specified date range. Each time the report is run you may not want the user to change the form name (HR11.1) but you will allow them to change the date range. Checking the Prompt at runtime checkbox will allow them to change the date each time the report is run.

### Exporting

#### **Creating a MS Excel Document**

There are 2 ways to export your results to Microsoft Excel. The Excel icon on each line will export the data related to the individual record selected. The Excel icon in the upper right corner of the screen will give you the option of exporting the entire search or just the page currently being displayed.



Select the version of Excel supported by your computer.

### Creating a PDF

There are 2 ways to export your results to a PDF file. The Adobe icon on each line will print the data related to the individual record selected. The Adobe icon in the upper right corner of the screen will give you the option of printing the entire search or just the page currently being displayed.



### Printing

The printer icon will function like any other browser page you need to print. This will only print the data on the current screen.

Saving Queries

### Saving a New Query

To save a report simply select the Save icon in the top right corner of the screen. Enter a report name and assign the report group for this report. The report group determines which users can view and run a saved report. The report groups are assigned on the administration page under Reporting Groups. Refer to the Kinsey Admin Guide for more information on defining and assigning user groups.

Save Report		×
Save new report as:	Vendor Master Chgs	
Assign to report group:	Finance •	
Cancel	Save	

# Saving an Existing Query

To save an existing report simply select the Save icon in the top right corner of the screen. You can save changes to an existing report by selecting SAVE in the Overwrite existing section. To create a new report from a copy of an existing report enter a new report name and assign the report group for this report in the Save new report section. The report group determines which users can view and run a saved report. The report groups are assigned on the administration page under Reporting Groups.

₩ Save Report		×
	Favorites: Shared Reports	
Overwrite existing?	AP10.1 Changes	
	Save	
Save new report as:		
Assign to report group:	Finance •	
Cancel	Save	

# Scheduling Reports

Scheduling a report will allow you to automatically create and email any report you would like to receive on a regular basis.

To schedule a report you must first create and save your report. Once the report displays in the left navigation pane right click on the report name and select **Schedule**.

Favorites Group Reports	<
Finance	AP10.1 Changes
Finance Users	Run Report
	<u>Rename</u>
Shared Reports	<u>Delete</u>
All HR11 Chang	Schedule
AP10.1 Change	s (U

A grey clock icon is displayed if a schedule already exist for a report but it is not enabled. A blue clock icon indicates the the schedule is currently enabled.

Schedule Repor	t	×
Select schedule to use: Schedule name: Every day at	<ul> <li>Select existing Create new schedule</li> <li>Every Morning •</li> <li>04 : 59</li> </ul>	
Select users to email: Email group name: d.kinsey@kinsey.com	<ul> <li>Select existing</li> <li>Create new group</li> <li>HR Dept</li> </ul>	1.
Email format: Send blank reports: Cancel	Adobe PDF (*.pdf) ▼	Save

The scheduling screen allows you to setup new schedules or use existing schedules. Schedules can be set to run each minute, hour, day, week, month or year.

You can also create or use existing report groups. A report group contains a list of users you want to receive the report.

Send report export to:

The export options are Excel or Adobe PDF

Send blank reports:

If you want the system to generate and send a report even if there is nothing to report select this option. This will inform the receipient that the report was run.

# **Deleting a Report**

To delete a report, select the report name and click on Delete. You must have the proper permissions to delete a report.

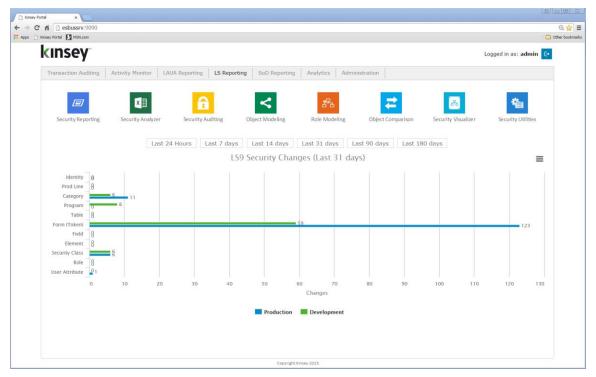
### **Renaming a Report**

To Rename a report, select the report name and click on Rename. You must have the proper permissions to rename a report.

# **Object Modeling**

The Object Modeling application provides a means to simulate a security change to a particular object and project the impact on a users security. The optional security objects are forms, tables or system codes. Additionally the application will check for any potential Segregation of Duties violations that may be created by the change.

Note: The Segregation of Duties (SoD) application is required to validate potential Sod violations.



Launch the Security Dashboard and select the Object Modeling icon from the LS Reporting tab.

Start by selecting the server and LDAP profile you want to report on in the top right corner of the screen.

Production Server	▼ * APS	· 🗎	?	ۥ
	Data L	ast Updated: :	12/3/1	4 14:43

### Search

To start the process simply enter the object in the search box that you would like to model. A dropdown list of matching objects will automatically be displayed as you start to type.

🗅 Kinsey Portal X 🗋 Kinsey Portal X 🗋 Kinsey Object Modeling X	
← → C n esbussrv:9090/KK_LS9ReportingPortal/what-if.htm?SERVERID=LSF_	_PROD&PROFILE=APS Q ☆ =
Apps 🔞 Kinsey ESBus Home Pa 🚺 MSN.com	C Other bookmarks
KINSEY <sup>-</sup> Cobject Modeling	Production Server • * APS • 🔒 ? ↔ Data Last Updated: 12/3/14 14:43
Search AP10	
Form/Executables	
AP10.1 - Vendor	
AP10.2 - Vendor Location	
AP10.3 - One Time Vendor	
AP10.4 - Customer	
AP10.5 - Vendor, Company Codes	
AP10.6 - Location, Company Codes	
AP10.7 - Vendor Approval	

Once you have selected the object you can then click on the **Find Affected Objects** button. The system will display a list of the Security Classes, Roles and Users that have access to this object..

*Note: the orange padlock icon next to the Task indicates that the object has ALL\_ACCESS. The function codes are displayed for additional modeling purposes.* 

C Kinsey F	Portal x	'' Kinsey Portal × Chi Kinsey Object Modeling	×				LE	
<b>←</b> → (	🕈 🏦 🗋 esbussrv:	9090/KK_LS9ReportingPortal/what-if.htm?SE	RVERID=LSF_PROD&PRO	FILE=APS				@ ☆ ≡
👯 Apps [	Kinsey ESBus Home Pa	MSN.com						Cther bookmarks
kı	nsey	Cbject Modeling			Produ	ction Server •	APS •	? (+
							Data Last Updated: 12/	3/14 14:43
Search	AP10.1							
Туре	S.	stem Code Name Description	# of SoD Rules					
	Executable AF		2	Due COD Depart				
10111/1			-	Run SOD Report				
Find	Affected Ob	jects						
		-						
Status	Task		Task Rule	Role	l	lser	Rule	
	VSS	Vendor Self Service	I,N,P	FinSup	- 1	rogers Rogers, Hal	ALL_ACCESS	
	MNitkaAdmin		P.N.I	GLAccountan	t- 1	nnitka Nitka, Mike	ALL_ACCESS	
	APSetup	Accounts Payable Setup Screens	A.C.D.I.N.P	VendorRole	- s	miller Miller, Saral	h ALL INQUIRES	
	Controller	Controller	1				-	
	zzAPInguiry	zzAPInguiry	ALL_INQUIRES					
l Y	22Ai inquiry		ALL_INGOINED					
		Add object to a Task						
Change								
Change	LOB							

The next step is to view the vairous routes a user might have to access this object. By clicking the either a Task (Security Class), Role or User the sytem will draw a map between objects.

In the example below the user *smiller* was selected. A blue line was drawn from *smiller* to the Role *GLAccountant* and then to the tasks associated with *GLAccountant* that contain the object AP10.1

C Kinsey F	fortal ×	'i Kinsey Portal × 🗋 Kinsey Ob	rject Modeling ×							
	Kinsey ESBus Home Pa		f.htm?SERVERID=LSF_PROD&PRO	FILE=APS						이, ☆ 클
	ısey	Cbject Mode	ling			F	roduction Se	rver • * A		? (+
		AP10.1 Ven	cription # of SoD Rules dor 2	Run SO	D Report	Object Relat		<u>Hide</u>	Data Last Updated	: 12/3/14 14:43
Status V V V V	Task VSS MNitkaAdmin APSetup Controller zzAPInquiry	Vendor Self Service Accounts Payable Setup S Controller zzAPInquiry <u>Add object to a Task</u>	I ALL_INQUIRES		Role FinSup - GLAccountant - VendorRole -		-	Rogers, Hal Nitka, Mike Miller, Sarah	Rule ALL_ACCESS ALL_ACCESS ALL_INQUIRES	
Change	Log									_

Similary you can click on the Task *APSetup* and see the associated Roles and Users associated with the task or select a Role and map to the Tasks and Users associated with the Role. You can cancel the mapping by clicking on the Hide link optIon on the legend.

Once you visually understand the mapping you can you multiple modeling options:

- 1. Remove the object from an assigned Task
- 2. Add the object to a new Task
- 3. Change a Task rule
- 4. Generate Security Reports based on the object selected
- 5. View potential Segregation of Duties violations.

### Removing an Object Assignment from a ExistingTask

To visually see the affect of removing an object from a Task simply click on the green check mark left of the Tasks list.

Start by clicking on APSetup to see how the object is assigned in security. You will notice that users hrogers and mnitka have ALL\_ACCESS

C Kinsey P	ortal ×	Kinsey Portal	× 🗅 Kin	sey Object Modeling	×								
		v:9090/KK_LS9Rep	portingPortal/w	hat-if.htm?SER\	VERID=LSF_PRO	D&PROF	ILE=APS						@,☆ ≡
Apps 😣	Kinsey ESBus Home Pa	MSN.com											C Other bookmarks
kır	ısey	* < o	Object Mo	deling					F	Production Se	erver • * /	APS •	? (+
	_											Data Last Update	ed: 12/3/14 14:43
Search	AP10.1								Object Relat				
Туре	s	ystem Code	Name [	Description	# of SoD R	ules			Tas	k - APSetup	<u>Hide</u>		
	xecutable A		AP10.1 \		2		Run SO	D Report					
							itan oo	bittoport					
Find	Affected Obj	iects											
Status					Task Rule			Role	_	User		Rule	
<ul> <li>Image: A set of the set of the</li></ul>	VSS	Vendor Se	If Service		I,N,P			<ul> <li>FinSup</li> </ul>		-	Rogers, Hal	-	
<ul> <li>✓</li> </ul>	MNitkaAdmi	in			P,N,I			GLAccount		mnitka	Nitka, Mike	ALL_ACCESS	
<b>~</b>	APSetup	Accounts P	Payable Setu	up Screens	A,C,D,I,N,P	ď	1	VendorRole		smiller	Miller, Sarah	ALL_INQUIRES	
<ul> <li>Image: A second s</li></ul>	Controller	Controller			I.								
<ul> <li>Image: A start of the start of</li></ul>	zzAPInquiry	zzAPInquir	γ		ALL_INQUI	RES							
		Add o	bject to a T	ask									
Change	Log												
							Copy	right (c) 2015					
L													

If you then click on the green checkmark next the the Tast APSetup you will see the rule permissions for hrogers and mnitka change to 'I' inquiry only

C Kinsey P	ortal ×	🛅 Kinsey Portal	×	Kinsey Object Modeling	×									
← → C	🕈 🏦 🗋 esbussrv	r:9090/KK_LS9Re	portingPortal	l/what-if.htm?SER	VERID=LSF_PRO	D&PROF	ILE=APS							@☆ 〓
🔛 Apps [8]	Kinsey ESBus Home Pa	MSN.com												C Other bookmarks
kır	ısey	. < 0	Object N	lodeling						Pr	oduction Se	rver • A	IPS •	? (+
													Data Last Update	ed: 12/3/14 14:43
Search	AP10.1									Object Relati	onships			
		the contra		Description	# - { C - D D					Task	- APSetup	<u>Hide</u>		
Туре		ystem Code			# of SoD Ru	lies								
Form/E	xecutable A	P	AP10.1	Vendor	2		Run SOI	D Report						
Find	Affected Obj	ects												
Status	Task				Task Rule			Role			User		Rule	
<ul> <li>Image: A second s</li></ul>	VSS	Vendor Se	If Service		I,N,P			FinSup	-		hrogers	Rogers, Hal	1	
<ul> <li>✓</li> </ul>	MNitkaAdmi	n			P,N,I			GLAccountant	i -		mnitka	Nitka, Mike	1.00	
×	APSetup	Accounts (	Payable Se	etup Screens	A,C,D,I,N,P	<b>a</b>		VendorRole	-		smiller	Miller, Sarah	ALL_INQUIRES	
	Controller	Controller			1									
	zzAPInguiry	zzAPInguir	v		ALL_INQUIF	RES								
· ·	. ,				_									
		Add c	bject to a	<u>a Task</u>										
Change	100													
-	ed security clas	cc: ADSetun												
Disable	a security tid:	ss. Ar Setup												
							Сору	right (c) 2015						

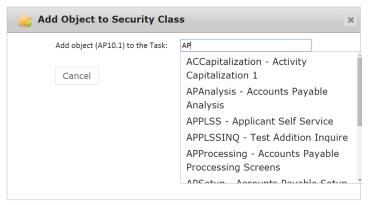
Anytime a users access level changes the new rule will turn to the color orange. To see why the user has this rule click on the user ID. The application will map the user to their available Tasks. In the example below the user *mnitka* also had access to AP10.1 through

the Controller task and thus receives Inquiry access. So deleting Task APSetup won't remove access for mnitka because Inquire access is provide through a different Task.

🗋 Kinsey P	fortal x	🗅 Kinsey Portal 🛛 🗙 🕒 Kinsey Object Modeling	×							
		9090/KK_LS9ReportingPortal/what-if.htm?SEI	RVERID=LSF_PROD&PRO	FILE=APS						@ ☆ =
Apps 🚷	Kinsey ESBus Home Pa	MSN.com								Cther bookmarks
kır	<b>isey</b> <sup>®</sup>	Object Modeling				Pro	duction Se	rver • * A	PS •	? (~
									Data Last Update	ed: 12/3/14 14:43
Search	AP10.1					Object Relatio				
Туре	Sy	stem Code Name Description	# of SoD Rules				APSetup	<u>Hide</u>		
	xecutable AF	AP10.1 Vendor	2	Run SO	D Report	User -	mnitka	<u>Hide</u>		
Find /	Affected Obje	ects								
Status	Task		Task Rule		Role		User		Rule	
<ul> <li>Image: A second s</li></ul>	VSS	Vendor Self Service	I,N,P		FinSup -		hrogers	Rogers, Hal	1. Contraction of the	
<ul> <li>Image: A second s</li></ul>	MNitkaAdmin	1	P,N,I		GLAccountant -		• mnitka	Nitka, Mike	1	
×	APSetup	Accounts Payable Setup Screens	A,C,D,I,N,P 🔐	1	VendorRole -		smiller	Miller, Sarah	ALL_INQUIRES	
<ul> <li>Image: A second s</li></ul>	Controller	Controller	1	1						
<b>~</b>	zzAPInquiry	zzAPInquiry	ALL_INQUIRES							
		Add object to a Task								
Change Disable	Log ed security clas	s: APSetup								
				Сору	right (c) 2015					

# Adding an Object to a New Task

To visually see the affect of adding an object to a new Task click on the "Add object to a **Task**" link. You will have the the option of entering the Task you would like to add the object to.



Note: This is only a model, no change is being made to security during this process.

The result of adding form AP10.1 to *ACCapitalization* shows 1 additional user and 1 additonal Role in the model and how adding the object will change the assigned users permissions.

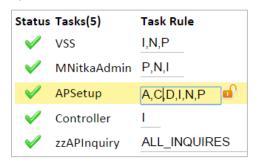
Rinsey Po	ortal ×	rey Portal ×	×						E	V D D X
		)/KK_LS9ReportingPortal/what-if.htm?SERVE	RID=LSF_PROD&PROF	FILE=APS						© ☆ ≡
Apps 🚷	Kinsey ESBus Home Pa 🚺 MS	N.com								Other bookmarks
kir	ısey	Cbject Modeling				Produ	iction Serve	er 🔹 * APS	- <b>i</b>	? (→
								Data	Last Updated: 12/	3/14 14:43
Search	AP10.1				C	bject Relations				
Туре	Svste	m Code Name Description	# of SoD Rules			Task - A		<u>lide</u>		
	xecutable AP		2	Run SOD R	eport	User - m	nnitka <u>I</u>	<u>lide</u>		
				Run SOD I	cepore					
Find A	Affected Objects									
Status	Task		Task Rule		Role		User		Rule	
<ul> <li>Image: A second s</li></ul>	VSS	Vendor Self Service	I,N,P		FinSup		hrogers	Rogers, Hal	1	
<ul> <li>Image: A second s</li></ul>	MNitkaAdmin		P,N,I		GLAccountant		mnitka	Nitka, Mike	A,C,D,I,N,P	
×	APSetup	Accounts Payable Setup Screens	A,C,D,I,N,P	s //	VendorRole	-	smiller	Miller, Sarah	ALL_INQUIRES	
<i>~</i>	Controller	Controller	1		ACExpert	-	lawson	Lawson, Lawson	A,C,D,I,N,P	
I	zzAPInquiry	zzAPInquiry	ALL_INQUIRES	;	ACAssetManager	-				
<ul> <li>✓</li> </ul>	ACCapitalization	Activity Capitalization 1	A,C,D,I,N,P	P						
		Add object to a Task								
Change	Log									
Disable	d security class: A	PSetup								
Added :	security class: A	CCapitalization								
				Copyrigh	nt (c) 2015					

# Changing a Forms Function Code Rule

This option give you the ability to see the affect of changing a rule on a Task . In the example below the maping indicates that 2 users have ALL\_ACCESS to form AP10.1 via the APSetup task.

🗋 Kinsey Po	ortal X	Kinsey Portal ×	Kinsey Object Modeling	×									
		srv:9090/KK_LS9ReportingPort	al/what-if.htm?SER	VERID=LSF_PRO	D&PROFILE	=APS							@ ☆] ≡
🔛 Apps 🙁	Kinsey ESBus Home Pa	MSN.com											Cther bookmarks
kır	isey	Cobject N	Modeling						Pro	duction Se	rver 🔹 🏝		? (~
												Data Last Update	ed: 12/3/14 14:43
			Description Vendor	# of SoD Ru 2		Run SOE	) Report		Object Relatio		<u>Hide</u>		
Status		Vanden Celf Camin		Task Rule			Role			User	Degree Hel	Rule	
	VSS	Vendor Self Service	•	I,N,P			FinSup	1		-		ALL_ACCESS	
<ul> <li>Image: A set of the set of the</li></ul>	MNitkaAdr	nin		P,N,I			GLAccountant	-		mnitka	Nitka, Mike	ALL_ACCESS	
<ul> <li>Image: A second s</li></ul>	APSetup	Accounts Payable S	etup Screens	A,C,D,I,N,P	<b>.</b>		VendorRole	-		smiller	Miller, Sarah	ALL_INQUIRES	
<b>~</b>	Controller	Controller		1									
~	zzAPInquir	y zzAPInquiry		ALL_INQUIF	RES								
		Add object to	a Task										
Change	Log												
						Copyr	ight (c) 2015						

To model the affect of changing the current rule simply click on the rule and a box will aprear.



At this point you can add additional function codeS or delete existing function codes.

C Kinsey	Portal ×	Kinsey Portal	× 🗋 Kinsey Objec	t Modeling ×									
€ ⇒ (	🗧 🏫 🗋 esbus	srv:9090/KK_LS9Report	tingPortal/what-if.h	tm?SERVERID=LSF	PROD&PROFI	LE=APS							© ☆ ≡
🔛 Apps 🚦	Kinsey ESBus Home Pa	MSN.com											Cther bookmarks
kı	ısey	C < Obj	ject Modeli	ng					Р	roduction Se	erver • * /	APS •	? 🗘
	-											Data Last Updat	ed: 12/3/14 14:43
Search	AP10.1							0	bject Relat	onships			
Туре		System Code N	ame Descr	iption # of So	) Rules			-	Task	- APSetup	<u>Hide</u>		
	Executable		P10.1 Vende			Run SO	) Report						
Find	Affected Ol	bjects											
Status	Task			Task Rule			Role			User		Rule	
<ul> <li>Image: A second s</li></ul>	VSS	Vendor Self S	ervice	I,N,P			FinSup		_	- hrogers	Rogers, Hal	A,C,I	
<ul> <li>Image: A second s</li></ul>	MNitkaAdn	nin		P,N,I			GLAccountan	t -		mnitka	Nitka, Mike	A,C,I	
<ul> <li>Image: A second s</li></ul>	APSetup	Accounts Pay	able Setup Sc	reens A,C,I		1	VendorRole	-		smiller	Miller, Sarah	ALL_INQUIRES	
	Controller	Controller		I.									
<ul> <li>Image: A start of the start of</li></ul>	zzAPInquiry	y zzAPInquiry		ALL_INC	UIRES								
		Add obje	ect to a Task										
Change	-												
Chang	ed security c	lass: APSetup from	m A,C,D,I,N,P	to A,C,I									
						Сору	ight (c) 2015						

When you tab out of the field the users new permission will be displayed.

Note: The system does NOT validate the available for function codes. Entering an invalid value will result in the appliation thinking the user now has this value.

Note: The application will display the "least restrive" access to the object you are working with. For example, if a user is assigned a Role that provides Inquiry only access and another Role that provides ALL\_ACCESS the users access will be displayed as ALL\_ACCESS (least restrictive) Additional Rule options that will be resolved correctly are:

- ALL\_ACCESS
- ALL\_INQUIRY
- ALL\_DELETE
- ALL\_ADD
- NO\_ACCESS

### Linking to Security Reports

This option gives you ability to drill directly to your security reports. By right clicking on any of the displayed objects you will have various reporting options.

C Kinsey P		Kinsey Portal	× 🗈 Kinsey Object I	m?SERVERID=LSF_PROD	PROFILE=	APS						Q☆≡
	Kinsey ESBus Home Pa		esperange or early more in the									Cther bookmarks
kır	ısey	<	Object Modelin	g					Production Se	rver • * A	PS • 💼	<b>?</b> (↔
Search	AP10.1										Data Last opdated.	12/3/14 14:43
	s xecutable A Affected Obj		Name Descrij AP10.1 Vendo			un SOD Repo	rt FinSup					
Status	Task VSS	Vendor S	elf Service	Task Rule I,N,P		Role FinSu		<u>Tasks</u> Task - Form -	User hrogers	Rogers, Hal	Rule ALL_ACCESS	_
<ul> <li></li> </ul>	MNitkaAdmi			P,N,I			countant	-		Nitka, Mike	-	
<ul> <li></li> </ul>	APSetup		Payable Setup Scr	eens A,C,D,I,N,P	<b>e</b>	Vende	orRole	-	smiller	Miller, Sarah	ALL_INQUIRES	
l 🎽	Controller zzAPInquiry	Controlle zzAPIngu		I ALL_INQUIRE	s							
		Add	object to a Task									
Change	Log											

In this example you can view the Tasks assigned to Role FinSup by selecting the Role – Task report.

🕒 Kinsey Portal	x 🖹 Kinsey Portal X 🖹 Kinsey	/ Object Modeling × 🕒 Lawson Securi	ty 9 Reporting X	
		rs.htm?SERVERID=LSF_PROD&	PROFILE=APS&ID=142&ROLEFILTER=FinSup	Q 🕁 :
Apps 🚷 Kinsey ESBus Home	e Pa 🚺 MSN.com			Cither bookman
kinse	Role - Task			첫 💷 Η 🛱 ? 🗠
Server: LSF_PROD	)   Profile: APS			Show Search Criteri
Expand Groups	Collapse Groups Clear	Filters		20 record
Drag a column ar	nd drop it here to group by th	at column		
Role		Task	Task Description	T 🔺
FinSup		AMProcessing	Asset Management Processing	
FinSup		AMSetup	Asset Management Setup	
FinSup		APProcessing	Accounts Payable Proccessing Screens	
FinSup		APSetup	Accounts Payable Setup Screens	
FinSup		Controller	Controller	
FinSup		DataAreaAccess		
FinSup		GLDataEntry	General Ledger Data Entry	
FinSup		GLProcessing	GL Processing for AP/GL Clerk	
FinSup		IFSubsystem	IF Subsystem	
FinSup		JournalEntry	JOURNAL ENTRY	
FinSup		MSAddQueryDist	MS Addin Query Only - Distribution Suite	
FinSup		MSAddQueryHR	MS Addin Query Only - HR Suite	
FinSup		POSetup	Procurement Setup and Upper Level Process	
FinSup		TESetup	Term Code Setup for Accounts Payable	
FinSup		TXSetup	Tax Setup for Accounts Payable	
FinSup		ACAnalysis	Activity Management Analysist Copyright (c) 2015	Ţ

# Viewing potential Segregation of Duties violations

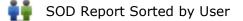
*Note: this option is only available if you have purchase the SOD application.* 

This option gives you ability to see if any of the changes you are considering would cause a violation to an SOD policy. When a task assignement or rule is changed as seen in the prior sections, the application will display the user new permission in orange. This is an indication that you may need to run the SOD report. The report will only work with the policies that contain the object being modeled.

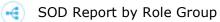
⇒ C & P eshussry	C Kinsey Portal × C Kinsey Object Model		)FILE=APS						Q 5
Apps 🕺 Kinsey ESBus Home Pa			ALL-AD						C Other book
kinsey	Object Modeling				Pro	duction Se	rver • * A	Data Last Updated	? 0
Find Affected Obje	P AP10.1 Vendor	on # of SoD Rules 2	Run SOD Rep	oort 📫		Ð	Object Relat		: 12/3/14 14
Status Task VSS MNitkaAdmir	Vendor Self Service	Task Rule I,N,P P.N.I	Role FinSu	p -			Rogers, Hal Nitka, Mike	Rule A,C,I A,C,I	
APSetup	Accounts Payable Setup Scree			orRole -				ALL_INQUIRES	
<ul> <li>Controller</li> <li>zzAPInquiry</li> </ul>	Controller zzAPInquiry <u>Add object to a Task</u>	I ALL_INQUIRES							
Change Log Changed security clas	ss: APSetup from A,C,D,I,N,P to /	ı,C	Copyright (c						

In the example above we can see that the function code rules were affected by the change to Tasks APSetup. This is an indication that the SOD report may need to be run.

Select the SOD Reporting link. Once the report is finished the application will display the following options.



SOD Report Sorted by Policy

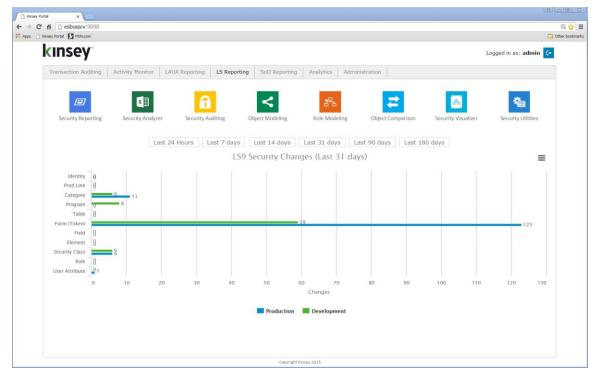




# **Role Modeling**

The Role Modeling application provides a means to simulate the affect on securty of changing a users Role assignment or changing the security classes assigned to a Role.

Launch the Security Dashboard and select the Role Modeling icon from the LS Reporting tab.



Start by selecting the server and Server you want to work with in the top right corner of the screen. The Profile will be based on the default set on the Admin Configuration page.

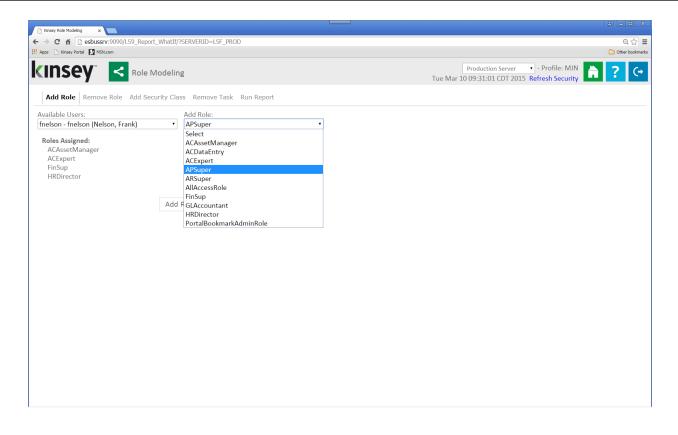
The following modeling options are available:

- Add a Role to a User
- Remove a Role from a User
- Add a Security Class to a Role
- Remove a Security Class from a Role

### Adding a Role to a User

Use this option if you want to review the affect of adding a Role to a users security settings.

On the Add Role tab select a user from the dropdown list. The application will display the Roles currently assigned to the user.



Using the Add Role dropdown select the Role you would like to add and click on the Add Role button. A list of your current selection is displayed in the top right corner of the screen. There is no limit to the number of changes you can model prior to running the report. For example, you can delete a Role from a user and add a different Role prior to running the security report.

Other options include removing a Role from User, adding a Security Class to a Role, and removing a Security Class from a Role.

Once you have finished your selections click on the Run Report tab. The application will launch the LS Security Analyzer reporting screen. From here you can run an saved report. For instructions on how to create a new report refer to the Securty Analzer section of this manual.

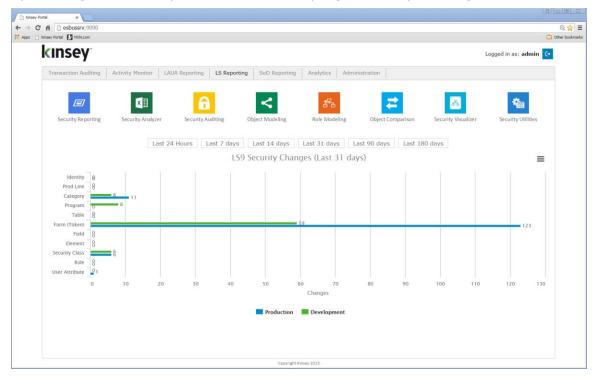
🕒 Kinsey Role Modeling 🛛 🗙 🔛				×
← → C fi C esbussrv:9090/LS9_Repor	t_WhatIf/?SERVERID=LSF_PROD		Q 🛣	Ξ
🔛 Apps 🗋 Kinsey Portal 🚺 MSN.com			Ci Other bookma	arks
Add Role Remove Role Add Sect			roduction Server • - Profile: MJN 🗎 ? C 19:31:01 CDT 2015 Refresh Security	
Saved Reports	✓ Role	Username (users that have roles attached)	✓ System Code	-
All  AM & HR  AM & HR  AM & HR  AM & HR - just FNELSON  AM & HR - just FNELSON  Financial Users  Finelson  GL45 Access  Finelson  Character  Ch	<ul> <li>ACAssetManager</li> <li>ACDataEntry</li> <li>ACExpert</li> <li>APSuper</li> <li>ARSuper</li> <li>AIRccessRole</li> <li>FinSup</li> <li>GLAccountant</li> <li>HRDirector</li> <li>PortalBookmarkAdminRole</li> </ul>	<ul> <li>✓ fnelson (Nelson, Frank)</li> <li>✓ hroberts (Roberts, Helen)</li> <li>✓ hrogers (Rogers, Hal)</li> <li>✓ lawson (Lawson Lawson)</li> <li>✓ Isadm (Lawson Admin)</li> <li>✓ Isuer (Lawson User)</li> <li>✓ mnitka (Nitka, Mike)</li> <li>✓ pfadmin (PFADMIN)</li> <li>✓ smiller (Miller, Sarah)</li> </ul>	<ul> <li>AC - Activity Management</li> <li>AD - Avg Daily Balance</li> <li>AM - Asset Management</li> <li>AP - Accounts Payable</li> <li>AR - Accounts Receivable</li> <li>BL - Billing</li> <li>BN - Benefits</li> <li>BR - AC Billing Revenue</li> <li>CB - Cash Ledger</li> <li>CW - Contract Work</li> <li>CX - Case Carts</li> <li>DT - Bills of Exchange</li> <li>EB - Budget Architect</li> <li>ED - EDI</li> <li>EE - Employee Expense</li> <li>EN - Enterprise Reporting</li> </ul>	
Form Conditional Rules	Report Name:			
<ul> <li>Table Access</li> </ul>				
Program Code Access	Query Description:			
<ul> <li>Field Rules</li> </ul>				
Field Conditional Rules	SAVE CANCEL			le.

The impact on a users security based on the changes made will be reflected in blue.

		Home	Insert Pac	j⊇ 🚰   🖛 je Layout Formulas Data Review Viev	w Developer	Add-Ins Acrobat				∞ 🕜 🗆	- 1
The	G12		• (e	▲ NO ACCESS	w Developei	Additis Actobat					8
2		А	В	С	D	E	F	G	Н	1	
				rson Access (LS9 Security) - Forms sers:Roles deleted from users:fnelsor	n = {ACExpert	}		Roles assigned to User ACAssetManager ACExpert HRDirector FinSup ARSuper			
	3							Users			
	4	Sys Code	Form ID	Title	Role	Security Class	Available Functions	fnelson			
	5	AC	AC00.1	Activity Group			A,C,D,I,N,P	I,N,P			
	9	AC	AC00.2	Calendar			A,C,D,I,N,P	I,TIME_RULE			
	13	AC	AC00.3	Activity Group Purge Status			C,I,N,P	I			
	16	AC	AC01.1	Mass Activity Copy			+,-,A,C,D,F,I,M,N,P,R,U,V,	NO_ACCESS			
	18	AC	AC01.2	Additional Parameters			NO FC	NO_ACCESS			
	20	AC	AC01.3	Inquire Filter			NO FC	NO_ACCESS			
	22	AC	AC01.4	Automatic Activity			A,C,D,I	NO_ACCESS			
	24	AC	AC01.5	Automatic Level			A,C,D,I	NO_ACCESS			
	26	AC	AC02.1	Status			+,-,A,C,I	I			
	30	AC	AC03.1	Resource			A,C,D,I,N,P	I			
	34	AC	AC03.2	AC Person Assignment			+,-,A,C,I,N,P	I			
	38	AC	AC03.3	HR Employee Assignment			+,-,A,C,I,N,P	I			
	42	AC	AC03.4	Vendor Assignment			+,-,A,C,I,N,P	I			
	46	AC	AC03.5	Asset Assignment			+,-,A,C,I,N,P	I			
	50	AC	AC03.6	Equipment Assignment			+,-,A,C,I,N,P	1			
	54	AC	AC03.7	Role Assignment			+,-,A,C,D,I,N,P	I			
	58	AC	AC03.8	Roles			+,-,A,C,I	I			
	62	AC	AC03.9	Resource Account			C,I	I			
	66	AC	AC04.1	GL Code			+,-,A,C,I	1			
	69	AC	AC05.1	Account Categories			NO FC	1			
	72	AC	AC06.1	Override Account Categories			+,-,C,I,N,P	I			
	76	AC	AC06.2	Override Mass Add/Change			A,C,I	I			

# **Object Comparison**

The Object Comparison application allows you to check for redundancies in your security model. By comparing every Role to everyother Role or every Task (security class) to every other Task you will get a visual representation of where you might have overlap. The intention of the application is to reduce redundancies in your security model. You should start by focusing on those objects that have a very hight smilar percentage.



Launch the Security Dashboard from your Windows browser and select the LS Reporting tab and select the Object Comparison icon. Start by selecting the server and LDAP profile you want to report on in the top right corner of the screen.



C Kinsey	Portal X 🗋 Kinsey Portal	X Kinsey Object Comparison X				<u> </u>
		eportingPortal/compare.htm?SERVERID=L	F_PROD&PROFILE=APS			@☆] ≡
	Kinsey ESBus Home Pa 🚺 MSN.com					C Other bookmarks
kir	ISEY 🔁 Objec	ct Comparison			Production Server   * APS	• 🗎 ? 😔
Compare	what? Roles • Compa	re objects Compare				Records: 792
⊽=	Role (a)		ommon Similarity (%) Objects		Absorbed (%)	^
+	HRClerical (10)	HRGeneralist (12)	9	69.2%		75.0%
+	HRGeneralist (12)	HRClerical (10)	9	69.2%		90.0%
+	CustomerRole (4)	RSSRequester (4)	3	60.0%		75.0%
+	RSSRequester (4)	CustomerRole (4)	3	60.0%		75.0%
+	SmartReconAdminRole (5)	SmartReconRole (3)	3	60.0%		100.0%
+	SmartReconRole (3)	SmartReconAdminRole (5)	3	60.0%		60.0%
+	EmployeeRole (5)	ManagerRole (6)	4	57.1%		66.7%
+	ManagerRole (6)	EmployeeRole (5)	4	57.1%		80.0%
+	HRDirector (20)	HRGeneralist (12)	11	52.4%		91.7%
+	HRGeneralist (12)	HRDirector (20)	11	52.4%		55.0%
+	ApplicantRole (3)	VendorRole (3)	2	50.0%		66.7%
+	ApplicantRole (3)	FinancialRole (3)	2	50.0%		66.7%
+	BRBiller (2)	BRReportingAdministrator (4)	2	50.0%		50.0%
			Previous 1 to 100	) Next		
			Copyright (c) 20	15		

You can then select to compare all Roles or all Tasks (Security Classes) from the dropdown selection. There are 2 levels of comparison for each object. When comparing Roles you can either compare Role/Task assignments or Role/Object assignments to all other Roles. When comparing Task you can compare Task/Object or Task/Rule to all other Tasks.

# **Comparing Roles-Tasks Assignments**

Once you have selected the server and profile select Roles from the 'Compare What?' dropdown window and then click on the compare button. The application will compare every Role to every other Role. The graph will reflect how similar the Role-Tasks assignments are and where one Role could completely absorb another Role.

→ C fi  esbussrv:9090/KK_LS	59ReportingPortal/compare.htm?SERVERID	=LSF_PROD&PROFILE=APS			Q 🖒
pps 🚦 Kinsey ESBus Home Pa 🚺 MSN.com					C Other bookn
(INSEY) 🔁 🕬	oject Comparison			Production Server   APS	🗔 🖬 🤶 🤇
npare what? Roles • Con	mpare objects Compare				Records:
Role (a) ⊽=	Role (b) ⊽=	Common Similarity (%) Objects		Absorbed (%)	
+ HRClerical (10)	HRGeneralist (12)	9	69.2%		75.0%
+ HRGeneralist (12)	HRClerical (10)	9	69.2%		90.0%
+ CustomerRole (4)	RSSRequester (4)	3	60.0%		75.0%
+ RSSRequester (4)	CustomerRole (4)	3	60.0%		75.0%
<ul> <li>SmartReconAdminRole (5)</li> </ul>	SmartReconRole (3)	3	60.0%		100.0%
Task Smart	ReconAdminRole SmartReconR	ole			
AllGENAccess	✓ ✓				
AIIRMAccess	✓ ×				
Bookmark	✓ ✓				
SMF Task: SMR	✓ ✓				
SMI Role   Task	✓ ×				
Task   Form					
+ Sma Task   All Objects	SmartReconAdminRole (5)	3	60.0%		60.0%
+ EmployeeRole (5)	ManagerRole (6)	4	57.1%		66.7%
	EmployeeRole (5)	4	57.1%		80.0%
-					

In this example you can see that the Role *SmartReconAdminRole* and *SmartReconRole* are 60% similar (green graph) By clicking on the plus sign left of the Role you can see how the Roles differ in their Task assignments. You can also drill to the the security reports for more information on a specific Task by simply clicking on the Task name.

The absorbtion graph (blue) indicates how much one Role can completely absorb another Role. In the example above you can see that all of the Tasks assigned to the *SmartReconRole* Role are also assigned to the *SmartReconAdminRole* Role.

# **Comparing Roles-Tasks Assignments at the Object Level**

The Compare Objects checkbox allows you to compare at a more granular level. For this comparison the application will compare how forms, categories, programs and tables are assigned to a Role.

Once you have selected the server and profile select Roles from the 'Compare What?' dropdown window, select the Compare Objects checkbox and then click on the Compare button. The application will compare every Role to every other Role. The graph will reflect

how similar the Role-Object assignments are and where one Role could completely absorb another Role.

	SBus Home Pa 🚺 MSN./	KK_LS9ReportingPortal/compare.h	IIII / SEKVERID	=LSF_PROD&PRO	DFILE=APS					⊙ i Other I
nsey	- 🔁 Object C	Comparison							Production Server	• 🗎 ?
e what? Ro	les 🔻 🗹 Compare	objects Compare								Recor
Role (a	)	Role (b)		ommon Similarity Dbjects	(%)			Absorbed (%)		
- SmartRe	econAdminRole (94)	SmartReconRole (90)		90			95.7%			100.0%
	rpe Object	Role (a) Task	Rule	Role (b)	Task	Rule	55.776			100.0%
CAT	AP	SmartReconAdminRole SMR	'ALL ACCESS'	SmartReconRole		'ALL ACCESS'				
CAT	cs	SmartReconAdminRole AllGENAccess	-	SmartReconRole		-				
CAT	IC	SmartReconAdminRole SMR	'ALL_ACCESS'	SmartReconRole		'ALL_ACCESS'				
CAT	IS	SmartReconAdminRole AllGENAccess	-	SmartReconRole	AllGENAccess	-				
CAT	LO	SmartReconAdminRole Bookmark	'ALL_ACCESS'	SmartReconRole	Bookmark	'ALL_ACCESS'				
CAT	MA	SmartReconAdminRole SMR	'ALL_ACCESS'	SmartReconRole	SMR	'ALL_ACCESS'				
CAT	PO	SmartReconAdminRole SMR	'ALL_ACCESS'	SmartReconRole	SMR	'ALL_ACCESS'				
CAT	RD	SmartReconAdminRole Bookmark	'ALL_ACCESS'	SmartReconRole	Bookmark	'ALL_ACCESS'				
CAT	SC	SmartReconAdminRole AllGENAccess	ALL_ACCESS'	SmartReconRole	AllGENAccess	'ALL_ACCESS'				
CAT	UN	SmartReconAdminRole AllGENAccess	'ALL_ACCESS'	SmartReconRole	AllGENAccess	'ALL_ACCESS'				
PDL	PDL\$_\$GEN	SmartReconAdminRole AllGENAccess	ALL_ACCESS'	SmartReconRole	AllGENAccess	'ALL_ACCESS'				
PDL	PDL\$_\$LIVE	SmartReconAdminRole SMR	'ALL_ACCESS'	SmartReconRole	SMR	'ALL_ACCESS'				
PDL	PDL\$_\$LOGAN	SmartReconAdminRole Bookmark	'ALL_ACCESS'	SmartReconRole	Bookmark	'ALL_ACCESS'				
PGM	LO12	SmartReconAdminRole Bookmark	'ALL_ACCESS'	SmartReconRole		'ALL_ACCESS'				
PGM	LO13	SmartReconAdminRole Bookmark	'ALL_ACCESS'	SmartReconRole		'ALL_ACCESS'				
PGM	L014	SmartReconAdminRole Bookmark	'ALL_ACCESS'	SmartReconRole		'ALL_ACCESS'				
PGM	LO15	SmartReconAdminRole Bookmark SmartReconAdminRole SMR	'ALL_ACCESS'	SmartReconRole		'ALL_ACCESS'				
PGM PGM	MA67 RD69	SmartReconAdminRole SMR SmartReconAdminRole Bookmark	'ALL_ACCESS'	SmartReconRole SmartReconRole		'ALL_ACCESS'				
PGM	UNUS	SmartReconAdminRole AllGENAccess	'ALL_ACCESS'	SmartReconRole		'ALL_ACCESS'				
PGM	UNPD	SmartReconAdminRole AllGENAccess	-	SmartReconRole		-				
PGM	UNPM	SmartReconAdminRole AllGENAccess	-	SmartReconRole		-				
RMO	Group	SmartReconAdminRole AllRMAccess	-	-						
RMO	Resource	SmartReconAdminRole AllRMAccess	-			-				
RMO	Role	SmartReconAdminRole AllRMAccess	-			-				
RMO	Structure	SmartReconAdminRole AllRMAccess	ALL ACCESS!							

In this example you can see that the Role *SmartReconAdminRole* and *SmartReconRole* are now 95.6% similar (green graph) in stead of 60% as reflected at the Role-Task level. By clicking on the plus sign left of the Role you can see how the Roles differ in their assignments. You can also drill to the the security reports for more information on a specific Obect by simply clicking on the Object ID.

The difference between the 2 Roles is hightlighted in pink.

Note: The Role Comparison option does not compare at the Rule level. This is a highlevel view of how objects are assigned to a Role and does not take form level access into consideration.

# **Comparing Tasks Assignments**

Once you have selected the server and profile select Tasks from the 'Compare What?' dropdown window and then click on the Compare button. The application will compare every

Task to every other Task. The graph will reflect how similar the Tasks object assignments are and where one Task could completely absorb another Task.

	Kinsey ESBus Home Pa	MSN.com	Object Compa	ison			Production Server   MJN	• 00her bi
par	e what? Task	(s •	Compare rules	Compare				Records: 2
7=	Task (a)	7=	Task (b)	Common Objects	Similarity (%)		Absorbed (%)	
+	AMUpdates(	01 (2)	AMUpdates02 (2)	2		100.0%		100.0%
-	AMUpdates(	02 (2)	AMUpdates01 (2)	2		100.0%		100.0%
	Object Type	Object	Task (a)	Rule	Task (b) Rule			
	CAT	AM	AMUpdates02	'ALL_ACCESS'	AMUpdates01 'ALL_/	ACCESS'		
	TKN	AM145	AMUpdates02	'ALL_ACCESS'	AMUpdates01 'I,J,M,	N,P,R'		
+	HRSetup03 (	2)	HRSetup04 (3)	2		66.7%		66.7%
+	HRSetup04 (	3)	HRSetup03 (2)	2		66.7%		100.0%
+	IFSetup00 (1	.41)	IFSetup01 (73)	73		51.8%		100.0%
+	IFSetup01 (7	3)	IFSetup00 (141)	73		51.8%		51.8%
+	APSetup00 (	90)	APSetup01 (42)	42		46.7%		100.0%
Ŧ		121	(00) 00001ta294	17		16 7%		AG 7%

In this example you can see that the Task *AMUpdates02* and *AMUpdates01* are 100% similar (green graph) at the Task-Object level. This level of reporting does not take the rule into account, only the object assignment. By clicking on the plus sign left of the Task you can see how the Tasks differ in their rule assignments. You can also drill to the the security reports for more information on a specific Object by right clicking on the Object name.

The absorbtion graph (blue) indicates how much one Task can completely absorb another Task. In the example above you can see that all of the Objects assigned to the AMUpdates02 Task are also assigned to the AMUpdates01 Task. This is not necessarily an indication that you can ellimiate a Task. At this point no comparison has been done at the Rule level.

# **Comparing Tasks Assignments at the Object Level**

The Compare Objects checkbox allows you to compare at a more granular level. For this comparison the application will compare how categories, programs, tables and rules are assigned to a Task.

Once you have selected the server and profile select Tasks from the 'Compare What?' dropdown window, select the Compare Objects checkbox and then click on the Compare button. The application will compare every Task to every other Task. The graph will reflect how similar the Task-Object assignments are and where one Task could completely absorb another Task.

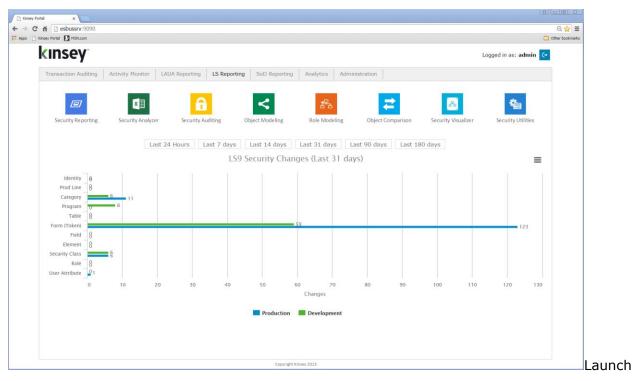
ps 📘	Kinsey ESBus Home Pa MSN.com	9ReportingPortal/compare.htm?SERV				ට, ද් Other boo
	nsey 🔁	Object Comparison			Production Server   MJN	- 🔒 ? 🤇
ipar	re what? Tasks 🔹 🖉	Compare rules Comp	are			Records: 27 (filte
7:	Task (a)		nmon Similarity (%) jects		Absorbed (%)	
-	AMUpdates01 (2)	AMUpdates02 (2)	1	33.3%		50.0%
	Object TypeObjectCATAMTKNAM145	Task (a)RuleAMUpdates01'ALL_ACAMUpdates01'I,J,M,N,				
+	AMUpdates01 (2)	AMMisc00 (2)	1	33.3%		50.0%
+	AMUpdates02 (2)	AMUpdates01 (2)	1	33.3%		50.0%
+	AMUpdates02 (2)	AMMisc00 (2)	1	33.3%		50.0%
+	AMUpdates01 (2)	AMPurges00 (5)	1	16.7%		20.0%
+	AMUpdates02 (2)	AMPurges00 (5)	1	16.7%		20.0%
+	AMUpdates01 (2)	AMInterfaces00 (8)	1 -	11.1%	-	12.5%
L.	AMIIndates()? (?)	AMInterfacec00 (8)	1	11 1%	_	17 5%

In this example you can see that the Task *AMUpdates02* and *AMUpdates01* now only 33% similar (green graph) in stead of 100% as reflected at the Task-Object level. By clicking on the plus sign left of the Task you can see how the Tasks differ in their assignments. You can also drill to the the security reports for more information on a specific Obect by right clicking on the Object ID.

The differences between the 2 Tasks are hightlighted in blue.

# **Security Visualizer**

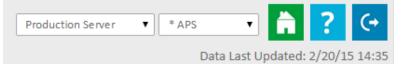
The Security Visualizer provides a graphical representation of your security model. You will be able to drill to security reports at either the User, Role or Security Class (Task) level. Additionally you can assign Roles to Users or Secutity Class to Roles and upload the changes to LS security provide you have valid credentials.



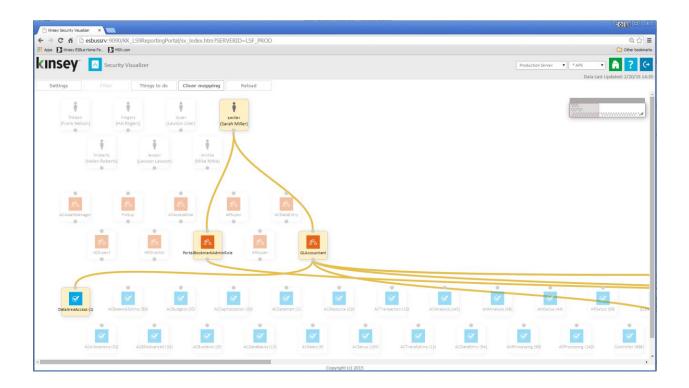
the Security Dashboard from your Windows browser and select the LS Reporting tab and select the Security Visualizer icon.

### Displaying a User Map

Start by selecting the server and LDAP profile you want to report on in the top right corner of the screen.



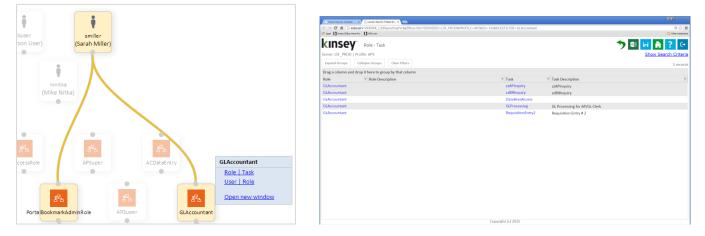
By defaut the application will display a map of the first 100 users in the system and their corresponding Role/Security Class assignments.



You can select an object at any of the 3 levels to view the assignments. In this example I select user 'smiller' to see the assigned Roles and Security Classes. I could have selected any of the Role to see the users are assigned or selected a Security Class to see the Role and User assignments.

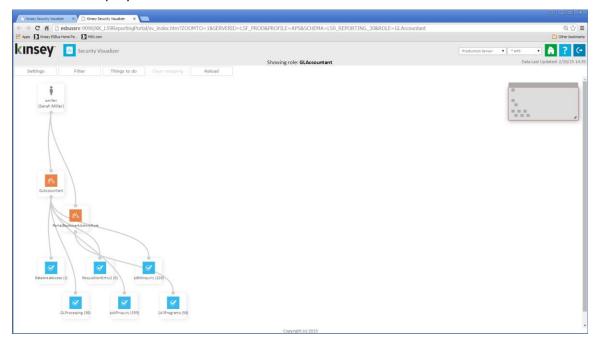
Once you have selected a map you can view specific security settings for any highlighted object.

The pop up window allows me to view this mapping in a new window or link to the security LS security reports..



When I selected a report link the appropriate LS report including the filters will be displayed on a new browser page.

If I select the Open New Window option the map will display all objects associated the with selected object. In this example the Role GLAccountant was only assigned to smiller, however had the Role been assigned to another user both users and their mapping would have been displayed.



### Settings

The settings buttom provides some default options for the current session.

🖌 Sett	ings	×
Hide se	elf-service users:	
Show r	node connections:	
Hide n	avigator:	
Show I	og:	
Maxim	um users to display:	100 🔻
	Save	

Hide self-service users: This option will be check by default. The application will look for specific settings in LDAP to determine which users are Self-Server and which are back office users.

- Show node connections: The node connections are the lines that lines that link objects when the map is displayed. By defaults the mapping is not displayed until you select a speicific object.
- Hide navigator: The navigator is used to quickly move to other sections of the map. The navigator window will be displayed in the top right corner of the page.



By dragging he grey shadowed section within the section the map will change orientations.

Show log: The option will display a list of any new or deleted assignments created during the session. The list of changes can then be upload to LDPA provided you have the proper credentials. This is explained in more detail in the Modifying Role Assignments and Modifying Security Class Assignments sections below.

Maximum users to display: The options are 50, 100, 250 or 500

# Applying Filters to a User Map

Filters will allow you to work with a smaller group of objects when displaying a map. The are 3 filters you can use prior to displaying the map:

- Users
- Role
- Task (Security Class)

The User filter provides 3 options; user name, group name or all users assigned a specific Role.

The Name option will use the full name of the user assigned in LDAP. This is not the users login ID. The filter logic uses a 'Contains' statement to select the users to display. So for example if I enter 'h' I will see a map for Helen Roberts, Sarah Miller and Hal Ragers. All 3 users have an 'h' in their name.

The Group and Has Role filters work the same way utilizing contains logic to build the map.

🐔 Filter Obj	jects ×							
User								
Not Selected 🔻								
Not Selected Name Group Has Role Task								
Not Selected <b>v</b>								
	Filter							

The Role filter is similar to the User filter but only provides one option.

The application will find all Roles that contain any part of what is entered. For example if I enter 'per' the Roles ACExpert, ARSuper and APSuper will be displayed.

Filter Objects	×
User	
Not Selected 🔻 a	
Role	
Not Selected 🔻	
Not Selected	
Name	
Not Selected 🔻	
Filter	

The Task (Security Class) filter is similar to the other two and provides a couple of options.

You can enter any part of a Task name and the application will use 'contains' logic to find matching Tasks.

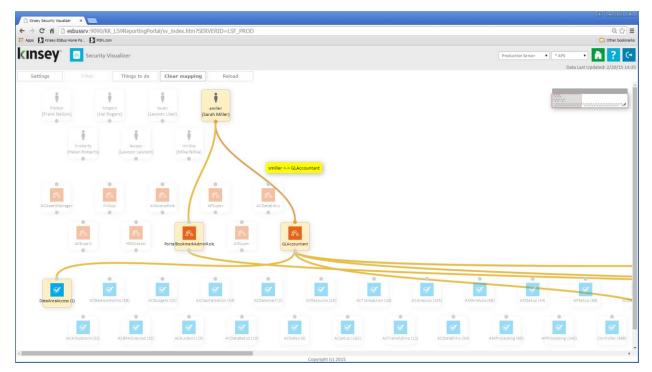
The Has Object option allows you to enter a specific form or table that might be contained in a Security Class. For example if HR11.1 is entered as the Object name all Users, Roles and Security Class linked to HR11.1 will be displayed.

🔏 Filter Obj	ects ×						
User							
Not Selected 🔻							
Role							
Not Selected 🔻							
Task							
Name 🔻							
Not Selected							
Name	Filter						
Has Object							

# **Modifying Role Assignments**

The application will allow you to either add or delete a Role assigned to a specific User.

*Note: The application will not allow any user with access to this feature to upload the changes to LDAP without the proper credentials.* 



To delete a Role, click on the line that connecs the User to the Role. You will received a message box asking you to confirm the delete. If you have logging turned on the action will be displayed in the log window.

Cancel

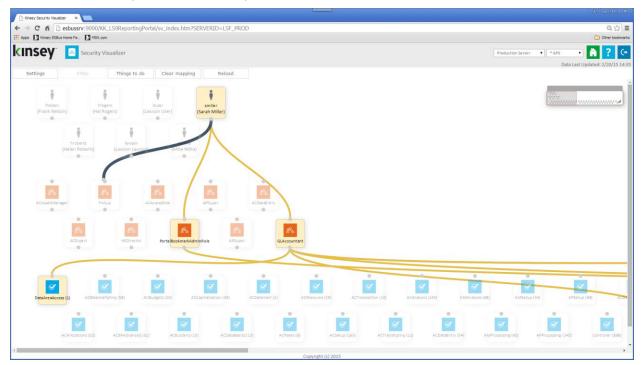
οк

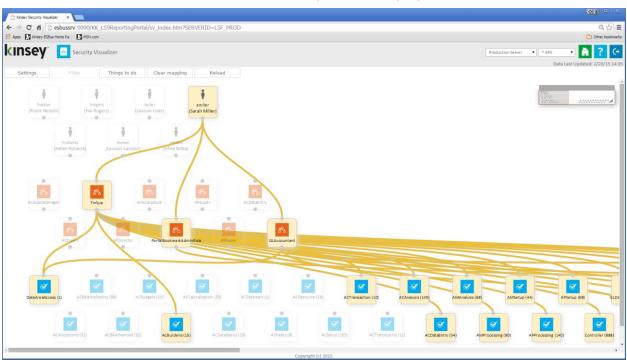
To upload the change click on the <u>Things to do</u> button.

Security Visualize	er			
Filter Th	ings to do Clear mapping	Reload		
	🐴 Utilities	×	Iawson Security	×
hrogers on) (Hal Rogers)	Upload changes to Lawson		LAWS <b>⊚</b> N"	
i			User Password	
hroberts Provided you have	the credentials to log in the	ne Lawson	Add ✔ Connection from "GLAccountant" (role) to "ACBurdens" (task)	

security administration tool the changes will be uploaded.

To assign a new Role to a User click on the small circle below the users name and draw a line between that point and the required Role.





Once the connection has been made a new map will be displayed.

To upload the change click on the <u>Things to do</u> button.

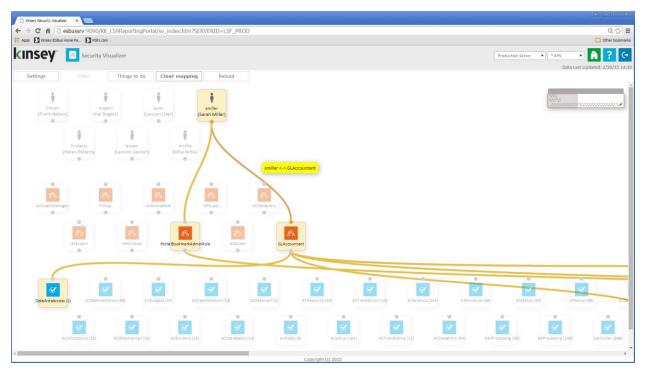
옪	Security Visualize	er	Lawson Security ×
Fi	lter Th	ings to do Clear mapping Reload	LAWS⊚N <sup>∞</sup>
	ŧ	Utilities 🗙	User Password
on)	hrogers (Hal Rogers)	Upload changes to Lawson	Add
hrobe	arte	lawson mnitka	OK Cancel

Provided you have the credentials to log in the Lawson security administration tool the changes will be uploaded.

### Modifying Security Class (Task) Assignments

The application will allow you to either add or delete a Task assigned to a specific Role.

*Note: The application will not allow any user with access to this feature to upload the changes to LDAP without the proper credentials.* 



To delete a Task, click on the line that connects the Role to the Task. You will received a message box asking you to confirm the delete. If you have logging turned on the action will be displayed in the log window.

To upload the change click on the <u>Things to do</u> button.

Sec	curity Visualizer		Lawson Security *
Filte	Thir	ngs to do Clear mapping Reload	LAWS
	hrogers	Utilities *	User Password
on)	(Hal Rogers)		Add Connection from "GLAccountant" (role) to "ACBurdens" (task) OK Cancel
hroberts		awson mnitka 🥑	

Provided you have the credentials to log in the Lawson security administration tool the changes will be uploaded.

To assign a new Task to a Role click on the small circle below the Role name and draw a line between that point and the required Task.

	Q 😭 🗎 Cotter boolmart tion Server • • *AP5 • • • • • • • • • • • • • • • • • • •
kinsey" Security Visualizer Produc	ction Server 🔹 🔹 🔹
Settings Filter Things to do Clear mapping Reload	ona con openedo si soj so so
freibun hungers Burer Statier (Frank Nelicon) (Hall Rogers) (Barson User) (Sarah Meller)	
Inderts     Issuen       (Helen Roberts)     Issuen       ACAsetMonager     Friso       ALAsetMonager     Friso	
ACCurat HIDreter PerialbookmanAdminRole ASser Concurant PortalbookmanAdminRole Statistics Concurant Concurat Concurant Concurant Concura	× ×
DerAkreakces (1) ACBeinner-Roting (58) ACBudgets (20) Concellation (33) ACDetement (2) ACResource (29) ACTransaction (13) ACAdesis (33) ACAdesis (43) AAAdesis (63) Concellation (32) ACBetavanced (32) ACBudgets (33) ACBetavanced (32) ACBetavanced	AMfetup (44) APletup (68) Controller (88)

finery Security Visualizer x	ALL X
← → C fi esbussry:9090/KK_LS9ReportingPortal/sv_index.htm?SERVERID=LSF_PROD	@☆ 〓
👬 Apos D Kinsey ESku Home Pa. D MSL.com	Cther bookmarks
KINSEY Security Visualizer	Production Server   * APS   APS
Settings Filter Things to do Clear mapping Reload	
freibon (Frank Neison) (Hal Rogers) (Lawson User) (Sarah Maller)	
Moderté wordh motités (Helen Roberto) (Lavison Lavison) (Mile Nitike) A CAser Manager Foto Alecensie Alecensie	
ACEsert Holivector Perta BookmanAdeminRole AEEsper	
DEFAVERANCES (1) ACSHIERCESTON (55) ACSHIERCESTON (53) ACCHARMENT (2) ACCHARMENT (2) ACCHARMENT (2) ACCHARMENT (2) ACCHARMENT (2)	AMAANyaa (68) AM5etua (44) A55etua (68) 5100
ACAllocations (32) ACBRAShamed (32) ACBranditis (32) ACBr	4) AMProcessing (50) APProcessing (140) Controller (888)
< Conscient (c) 2015	

Once the connection has been made a new map will be displayed.

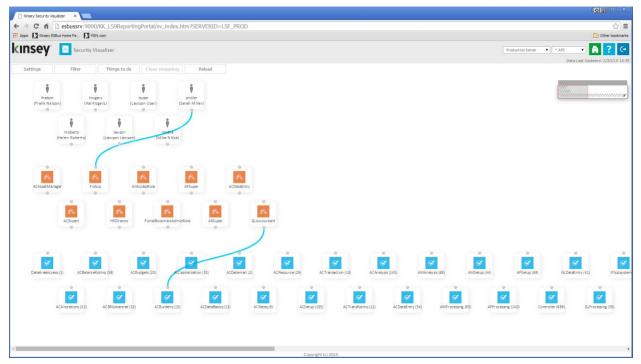
To upload the change click on the <u>Things to do</u> button.

🙈 S	Security Visualizer			With Lawson Security	×
Filt	ter Things	to do Clear mapping	Reload	LAWS@N <sup>*</sup>	
	hrogers	Utilities	×	User Password	
	(Hal Rogers)			Add Connection from "GLAccountant" (role) to "ACBurdens" (task)	
hrober				OK Cancel	

Provided you have the credentials to log in the Lawson security administration tool the changes will be uploaded.

# **Clear Mapping**

The Clear Mapping button wil give you a fresh start on making new assignments. When you clear the map any pending assignments will still be displayed. As you can see in this example the 2 changes made in the prior examples are still shown because they have not been uploaded to LDAP.



You can clear all pending LDAP changes by clicking on the Reload button or you can upload all the changes at once by selecting the Things to do button.

# **Security Utilities**

The Security Utility will allow you to ceate a inquiry only verions of an existing Security Class provicd you have the credientials to log into the Lawson Security Admin tool.

insey								Lo	gged in as: admin 🤆	
Transaction Auditing	Activity Monitor	LAUA Reporting	5 Reporting SoD	Reporting Ana	lytics Admi	nistration				
Security Reporting	Security Analyzer	Security Audition	ng Object Me		<b>辞</b> le Modeling	Object Compa		क्षेत्र y Visualizer	Security Utilities	
	Las	24 Hours Last	7 days Last 1	4 days Last :	31 days L	ast 90 days	Last 180 days			
			LS9 Securi	ty Changes (I	Last 31 da	ys)			=	
Identity 6 Prod Line 8 Category Program 0 Table 8 Form (Token) Field 8 Element 8 Security Class 8	8 11 8			<b>5</b> 9					123	
User Attribute	10 20	30	40 50	60 Chai	70 nges	80	90 100	110	120 130	
			Pr	oduction 📕 De	velopment					
Role 8 User Attribute 91	∎B 10 20	30		Cha	nges	80	90 100	110	120 130	

Select the LS Reporting tab from the Security Dashboard and choose the Security Utilities icon.

Start by selecting the server and LDAP profile you want to report on in the top right corner of the screen.

Production Server	ñ	?	(→	
-------------------	---	---	----	--

Select the "Clone a task to a 'read-only' task option.

The application will require you to enter your Lawson Security Administrator credentials.

i Laws	Lawson Security x							
	LA	WS⊚N <sup>™</sup>						
U Passw	lser							
[	ОК	Cancel						

Next select theTask (Security Class) you would like to clone from the dropdown selection list.

Kinsey LS Reporting X Lawson Securit	ty 9 Reportiny x 🗅 Kinsey Security Utilities x	A	- • ×
	9ReportingPortal/util_index.htm?SERVERID=LSF_PROD		् ☆ ≡
Apps 🗋 Kinsey Portal 🚺 MSN.com			Other bookmarks
kinsey	Security Utilities Production Server • * APS •	?	(→
Clone a task t	o a "read-only" task		
<b>T</b>	ACAnalysis - Activity Management Analysist	Task Det	ails
Task to clone	Refresh	System Codes	0
New task name:	AC Analysis RO	Program Codes	10
New task	AC Analysis Read Only	Tables	4
description:	no mary so nead only	Forms	91
Create		Fields	1
Create		Misc	39
	Copyright (c) 2015		

Enter the new Task (Security Class0) Name and Descripion and select the Create button.

# **Trouble Shooting**

### Why don't my security reports reflect my current changes?

The security reports use data from SQL tables that are updated nightly. Any security changes made during the day will be reflected the following day. To see your changes immediatedly you will need to run the scheduled task manually from the admin panel. For more information on how to run this task refer to the Kinsey Admin Users Guide, Scheduled Task.

# Why are the Form Names not displaying on my reports?

This happens when the Kinsey SQL metadata tables have not been updated. The Kinsey server uses the "Lawson" account to update the metadata tables. That account must be an LAUA (CHECKLS=NO) for our product to work correctly.

# Why are the Function Codes not displaying on my reports?

This happens when the Kinsey SQL metadata tables have not been updated. The Kinsey server uses the "Lawson" account to update the metadata tables. That account must be an LAUA (CHECKLS=NO) for our product to work correctly.

### Why doesn't the SOD report show conflicts that I know exist for some users?

The SOD Reports use the Security profile defined on the Admin Configuration page. Verify that the LS Security Configuration (Prod and Test) is referencing the correct profile name.

Notes: