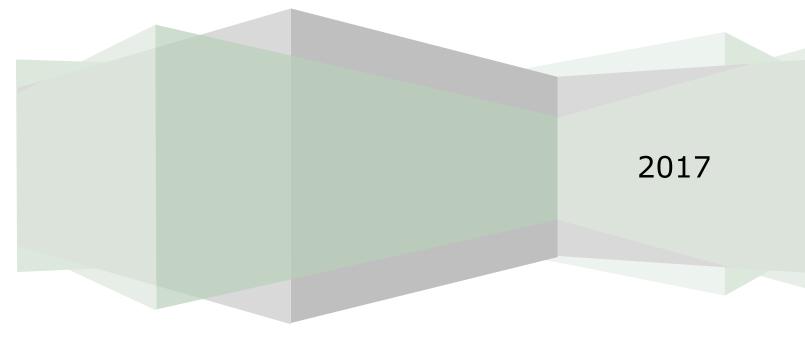


# Security Dashboard Users Guide

Security Reporting Security Analyzer Security Auditing Object Modeling Object Comparison Security Visualizer



# Contents

Setting your Default Home Page	5
Configuring your LDAP Reporting Profile	
Lawson LDAF Server Settings	0
Security Reports	7
Pre-Report Filters	9
Adding or Removing Selected Values1	1
Adding or Dropping All Values12	2
Adding or Removing Criteria Based Filters1	3
Historical Comparisons14	
Changing Pre-Report Filters1	5
Showing and Hiding Columns	
On-The-Fly Report Filters1	7
Grouping18	
Creating a Group18	
Grouping - Nested	
Grouping – Expand, Collapse or Remove	
Grouping – Remove Filters2	
Sorting	
Adding a Sort Option	
Removing the Sort Option	
Saving Reports	
Saving New Security Reports	
Changing and Saving an Existing Report	
Running Saved Report	
Exporting and Printing	
Drilling	
Historical Reports & Comparisons	
Comparing Profiles	
Scheduling Security Reports	
Deleting a Report	0
Security Analyzer	0
Selecting a Server	
Refreshing Your Data	
Creating a New Report	
Running an Saved Report	
Editing a Saved Report	
Deleting a Saved Report	
Reading the Analyzer Report	
Users Assigned Roles	
Assigned Forms (TKN)	
Assigned Roles and Security Classes	
Assigned Form Conditions	

Change Audit Reporting
Quick Search
Advanced Search
Prompt at Runtime
Exporting41
Creating a MS Excel Document41
Creating a PDF41
Printing
Saving a New Query
Saving an Existing Query
Scheduling Reports
Deleting a Report
Renaming a Report
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 DOLEDINAL SECTEDATION OF DUTLES VIOLATIONS
Viewing potential Segregation of Duties violations53
Role Modeling
Role Modeling
Role Modeling
Role Modeling       55         Adding a Role to a User       55         Object Comparison       58         Comparing Roles-Tasks Assignments       59
Role Modeling       55         Adding a Role to a User       55         Object Comparison       58         Comparing Roles-Tasks Assignments       59         Comparing Roles-Tasks Assignments at the Object Level       60
Role Modeling       55         Adding a Role to a User       55         Object Comparison       58         Comparing Roles-Tasks Assignments       59         Comparing Roles-Tasks Assignments at the Object Level       60         Comparing Tasks Assignments       62
Role Modeling       55         Adding a Role to a User       55         Object Comparison       58         Comparing Roles-Tasks Assignments       59         Comparing Roles-Tasks Assignments at the Object Level       60
Role Modeling       55         Adding a Role to a User       55         Object Comparison       58         Comparing Roles-Tasks Assignments       59         Comparing Roles-Tasks Assignments at the Object Level       60         Comparing Tasks Assignments       62         Comparing Tasks Assignments at the Object Level       63
Role Modeling       55         Adding a Role to a User       55         Object Comparison       58         Comparing Roles-Tasks Assignments       59         Comparing Roles-Tasks Assignments at the Object Level       60         Comparing Tasks Assignments       62         Comparing Tasks Assignments at the Object Level       63         Security Visualizer       64
Role Modeling       55         Adding a Role to a User       55         Object Comparison       58         Comparing Roles-Tasks Assignments       59         Comparing Roles-Tasks Assignments at the Object Level       60         Comparing Tasks Assignments       62         Comparing Tasks Assignments at the Object Level       63         Security Visualizer       64         Displaying a User Map       65
Role Modeling       55         Adding a Role to a User       55         Object Comparison       58         Comparing Roles-Tasks Assignments       59         Comparing Roles-Tasks Assignments at the Object Level       60         Comparing Tasks Assignments       62         Comparing Tasks Assignments at the Object Level       63         Security Visualizer       64         Displaying a User Map       65         Settings       67
Role Modeling       55         Adding a Role to a User       55         Object Comparison       58         Comparing Roles-Tasks Assignments       59         Comparing Roles-Tasks Assignments at the Object Level       60         Comparing Tasks Assignments       62         Comparing Tasks Assignments at the Object Level       63         Security Visualizer       64         Displaying a User Map       65         Settings       67         Applying Filters to a User Map       68
Role Modeling       55         Adding a Role to a User       55         Object Comparison       58         Comparing Roles-Tasks Assignments       59         Comparing Roles-Tasks Assignments at the Object Level       60         Comparing Tasks Assignments       62         Comparing Tasks Assignments at the Object Level       63         Security Visualizer       64         Displaying a User Map       65         Settings       67         Applying Filters to a User Map       68         Modifying Role Assignments       69
Role Modeling       55         Adding a Role to a User       55         Object Comparison       58         Comparing Roles-Tasks Assignments       59         Comparing Roles-Tasks Assignments at the Object Level       60         Comparing Tasks Assignments       62         Comparing Tasks Assignments at the Object Level       63         Security Visualizer       64         Displaying a User Map       65         Settings       67         Applying Filters to a User Map       68         Modifying Role Assignments       69         Modifying Security Class (Task) Assignments       72
Role Modeling       55         Adding a Role to a User       55         Object Comparison       58         Comparing Roles-Tasks Assignments       59         Comparing Roles-Tasks Assignments at the Object Level       60         Comparing Tasks Assignments       62         Comparing Tasks Assignments at the Object Level       63         Security Visualizer       64         Displaying a User Map       65         Settings       67         Applying Filters to a User Map       68         Modifying Role Assignments       69
Role Modeling       55         Adding a Role to a User       55         Object Comparison       58         Comparing Roles-Tasks Assignments       59         Comparing Roles-Tasks Assignments at the Object Level       60         Comparing Tasks Assignments       62         Comparing Tasks Assignments at the Object Level       63         Security Visualizer       64         Displaying a User Map       65         Settings       67         Applying Filters to a User Map       68         Modifying Role Assignments       69         Modifying Security Class (Task) Assignments       72
Role Modeling55Adding a Role to a User55Object Comparison58Comparing Roles-Tasks Assignments59Comparing Roles-Tasks Assignments at the Object Level60Comparing Tasks Assignments62Comparing Tasks Assignments at the Object Level63Security Visualizer64Displaying a User Map65Settings67Applying Filters to a User Map68Modifying Role Assignments72Clear Mapping75

# Introduction

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

The security reports are designed to help with the administration of Lawson Security with 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 report 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**

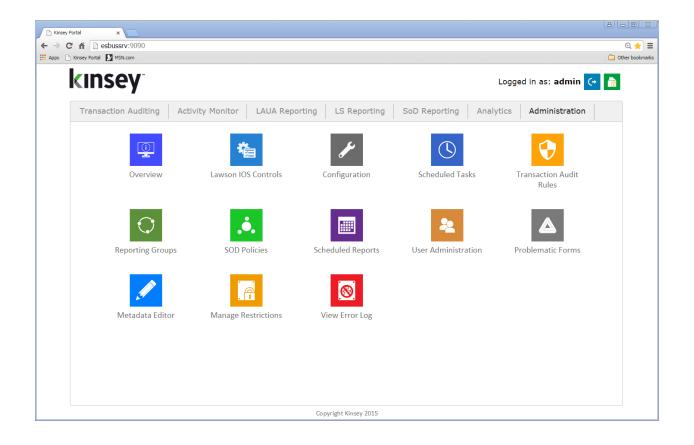
You can set your preferred Home page on the dashboard by selecting the home page icon in the top right corner of your screen. This setting is saved as a browser cookie and will be lost whenever you clear your browser cache.

# **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.

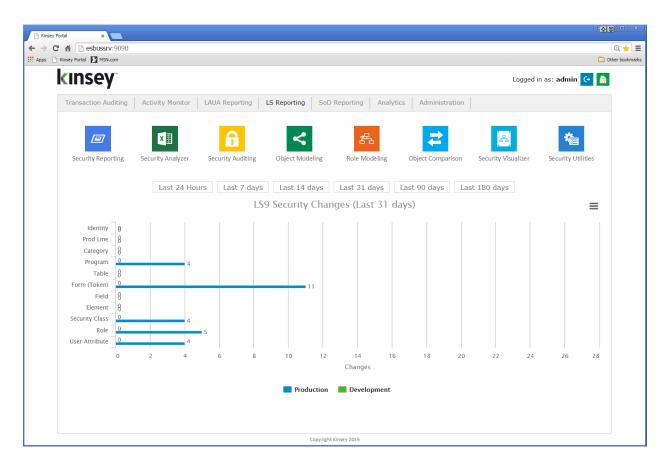
Examples of the fields generally used are: COMPANY, EMPLOYEE, HIRED and TERM\_DATE

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

# **Security 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 security 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 historical snapshots. Historical snapshots can be created through the administration panel. Refer to the Kinsey Administrator Guide, page 12, Schedule Tasks for more information.

Production Server				
★ Kney LS Reporting     ×       ← → C     © etbussn-6000/RCL/LS9ReportingPortal/       III Apps     ★ Kney Portal       KINSEY     ☑       Security Reporting     ☑	SERVERID-LSF_PROD&PROFILE=APS	ta Last Updated: 12/	S/ 14 14.43 Set as default Production - LS3SERVER	<ul> <li>- σ ×</li> <li>Q 2</li> <li>Other boolmarks</li> <li>* Ap5 * Inf</li> <li>? C</li> </ul>
Lerrs Lorse Lorse Labeled User - Attributes Disabled User - Attributes Disabled User - Attributes Disabled User - Identity User - All Objects User - All Objects User - Identity User - Identity User - Role - Group User - Role - Group User - Role - Security Class - Form User - Role - Security Class - Form User - Attribute Settings User - CheckLS & Not Set User - CheckLS Setting Users	Role - Security Class Role - Security Class - All Objects Role - Security Class - Eliment Group Role - Security Class Counts Role - Security Class Counts Role - Vier Counts Role - User Counts Roles Without Vases	Ecurity Classes Forms Per Security Class Security Class - All Objects Security Class - Rement Group Security Class - Remented Forms Security Class - Repeated Tables Security Class - Repeated Tables Security Class - Repeated Tables Security Class - Tables Par Security Class - Tables Tables Per Security Class Unassigned Objects Unassigned Security Classes	Statistics Metadata - Form Keys Metadata - Forms - Fords Metadata - Forms - Fords Metadata - Tables Structures Structures Metadata - Tables Structures - Olidien Structures - Olidien Struct	Data Last Updated: 6/9/17 11:32 Listener ** Activity lacking Security Form Count Summary User - Form Summary User - Form Summary User - Last Active User - No Activity Users Security versus Activity
LS Auditing ON LS Auditing - Location DB LS Auditing - Types ADD,CHG,DEL,SSO	Security Configuration Security Checking ON ProdUne/SysCad Action LVVE/AC ON LVVE/AZ OFF/NO_ACCESS MIN ON MIN/CW OFF/ALL_ACCESS	0 100 20	Unassigned Objects Object types not used in security my	odel 700 800 900 1100

The Security Reporting dashboard comes preconfigured with reports by User, Role, Security Class and 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.

Kinsey LS Reporting x Kole - Security Class - Fo x	▲ – □ ×
C O esbussrv:9090/KK_LS9ReportingPortal/filters.htm?SERVERID=LSF_PROD&PROFILE=APS&ID=141	९ 🕁 🖸 :
III Apps 🗶 Kinsey Portal	Other bookmarks
Role - Security Class - Form	🁈 🖥 🤶 어
Server: LSF_PROD   Profile: APS	<u>Hide Search Criteria</u>
Field Selection	
Role All T	
Security Class All	
Form All T	
Run a historical comparison	
Compare profiles	
Run Report	

For example, on the Role – Security Class – Form report you will have the option of filtering by Role, 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 Security Class 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 BetweenDate 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. This option can take a little time to populate depending on the size of the model. The values shown are based on the information available in your security model.

Kinsey LS Reporting X Kale - Security Class - Fo X		≜ – ⊡ ×
← → C ① esbussrv:9090/KK_LS9ReportingPortal/filters.htm?SERVERID=LSF_PROD&PROFILE=APS&ID=14	41	Q 🕁 🚺 🗄
III Apps Kinsey Portal		Cther bookmarks
<b>kinsey</b> <sup>*</sup> Role - Security Class - Form		🏷 🔒 ? 🤆
Server: LSF_PROD   Profile: APS		Hide Search Criter
Field Selection		
Role Advanced 🔻		
Available		Selected
ACAssetManager	Select Role	
ACDataEntry	Add > < Remove	
ACExpert		
AllAccessRole AllAccessRole	Add All >> << Remove All	
APInquery		
ApplicantRole		
APSuper	Contains 🔻	
ARSuper test description		
BRBiller		
BRContractAdministrator	Add > < Remove	
BRExpert	_	
RRReportingAdministrator Available: 4	10	Selected:
Security Class All		
Security class All		
Form All V		
Run a historical comparison		
Compare profiles		
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 LS Reporting X Role - Security Class - Fo X		≜ – □ ×
← → C ③ esbussrv:9090/KK_LS9ReportingPortal/filters.htm?SERVERID=LSF_PROD&PROFILE=APS&ID=141		० 🕁 🗖 🗄
III Apps Kinsey Portal		Other bookmarks
Role - Security Class - Form		🁈 🛃 🕻 🤇
Server: LSF_PROD   Profile: APS		Hide Search Criter
Field     Selection       Role     Advanced		
Available		Selected
EntryClerk	Select Role	
FinancialRole	Add > < Remove	
FinSup		
GLAccountant	Add All >> < Remove All	
GLReportWritter		
GLSuper	Contains V	
HRClerical	Contains 🔻	
HRDirector		
HRGeneralist	Add > < Remove	
ManagerRole		
OESalesOrderClerk	-	
Available: 40		Selected:
Security Class All		
Form All 🔻		
Run a historical comparison		
Compare profiles		
Run 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.

*Tip: There may be time where it's easier to add all and then remove the values you don't want selected rather that selecting a large list for inclusion.* 

Kinsey LS Reporting X Role - Security Class - Fo X			≜ – □ ×
← → C ③ esbussrv:9090/KK_LS9ReportingPortal/filters.htm?SERVERID=LSF_PROD&PROFILE=APS&ID=14	1		० 🕁 🖬 🗄
III Apps Kinsey Portal			Other bookmarks
Role - Security Class - Form			🏷 🔒 ? G
Server: LSF_PROD   Profile: APS			<u>Hide Search Criter</u>
Field     Selection       Role     Advanced			
Available			Selected
EntryClerk	^ Se	lect Role	
FinancialRole	Add >	< Remove	
FinSup			
GLAccountant	Add All >>	<< Remove All	
GLReportWritter		-	
GLSuper		ntains 🔻	
HRClerical	Cor	itains 🔻	
HRDirector			
HRGeneralist	Add >	< Remove	
ManagerRole	Add	< Remove	
OESalesOrderClerk	-		
Available: 4	0		Selected:
Security Class All			
Form All <b>v</b>			
<ul> <li>Run a historical comparison</li> <li>Compare profiles</li> </ul>			
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 LS Reporting X Kole - Security Class - Fo X		▲ - □ ×
$\leftarrow$ $\rightarrow$ C 0 esbussrv:9090/KK_LS9ReportingPortal/filters.htm?SERVERID=LSF_PROD&PROFILE=APS&ID=141		ዲ 🕁 🖬 🗄
Apps Kinsey Portal		Other bookmarks
Role - Security Class - Form Server: LSF_PROD   Profile: APS		Hide Search Criter
Field Selection		
Role Advanced V		
Available		Selected
EntryClerk	Select Role	ACAssetManager
FinancialRole	Add > < Remove	ManagerRole POPurchasingManager
FinSup		Populchasingivianagei
GLAccountant	Add All >> < Remove All	
GLReportWritter		
GLSuper	Contains	
HRClerical	Contains 🔻	
HRDirector	manager	
HRGeneralist	Add > < Remove	
OESalesOrderClerk	Adu >	
ONLYACDataEntry ONLY ACDataEntry Class		
Available: 37		Selected:
Security Class All		
Form All 🔻		
Run a historical comparison		
Compare profiles		
Run Report		

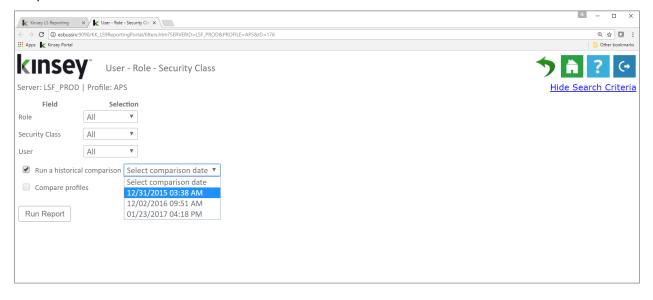
There are 2 options on which you base your logic; Contains and Starts With. In this example I will select "Contains", enter the value of "manager" and select the **Add** > button. As you can see all of the Roles containing "manager" in their ID or name have been moved to the selected list. You can remove 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 to determine the time and date of any security changes and/or 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 stamp you would like to compare against. 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 historical 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.

K Kinsey LS Reporting X / K User - Role - Security Cli X	≜ – □ ×
C O esbussrv9090/KK_LS9ReportingPortal/filters.htm?SERVERID=LSF_PROD&PROFILE=APS&ID=176	Q 🕁 🚺 🗄
III Apps 🖡 Kinsey Portal	Cther bookmarks
User - Role - Security Class	→ 1 ? <
Server: LSF_PROD   Profile: APS	Hide Search Criteria
Field     Selection       Role     All	
Security Class All 🔻	
User All T	
Run a historical comparison	
Compare profiles	
Run Report	

#### **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.

awson IOS Controls	LDAP Server:	s3server.co	pronet.lawson.com	
onfiguration	LDAP Port:	389		
cheduled Tasks	LDAP Base Search:	CN=lwsn,D	IC=ls3server	
ransaction Audit Rules	User LDAP Base Search:			
eporting Groups	LDAP Paging Size:	1000		
OD Policies	LDAP "back-office" Service:			
cheduled Reports	Collect Employee termination data:	<b>√</b>		
ser Administration	Employee fields to collect:	COMPANY	;EMPLOYEE;DATE_HIR	ED;TERM_DAT
roblematic Forms	LS Security Reporting Fields:		Friendly Name	Database Field
letadata Editor			Attribute	ATTRIBUTE
lanage 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

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

The second option allows you to change the columns displayed once the grid is populated. 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 and drop it here to group by that column											
User	T Full Name	▼ n-l- ▼ T-l.									
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	<ul> <li>Form</li> </ul>									
hroberts	Roberts, Helen	<ul> <li>Form Description</li> </ul>									
hroberts	Roberts, Helen	<ul> <li>Available FC</li> </ul>									
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.

Kinsey LS Reporting ×	Role - Security Class - Fc ×						<u>▲</u> – □
$\leftrightarrow$ $\rightarrow$ C 🛈 esbussrv:909	0/KK_LS9ReportingPortal/filters.htm?SERVERID=LSF	_PROD&PROFILE=APS&II	JD=141				@☆ 🖸
Apps 🕻 Kinsey Portal							📙 Other bookma
kınsey	Role - Security Class - Fo	orm			<b>→</b> 🖷	א א	<b>?</b> 🤆
Server: LSF_PROD	Profile: APS					<u>Show</u>	/ Search Criter
Expand Groups	Collapse Groups Clear Filters	Show/Hide	Columns				5,545 recor
Drag a column and	drop it here to group by that colu	mn		6			
Role	Y Role Description Y	Security Class	Y Security Class DescriptY	Form	Y Form Description Y	Available FC	Rule
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC00.2	Calendar	A,C,D,I,N,P	var zz=new ml
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC02.1	Status	+,-,A,C,I	'C,I,+,-'
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC03.1	Resource	A,C,D,I,N,P	'I'
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC03.2	AC Person Assignme	+,-,A,C,I,N,P	T
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC03.3	HR Employee Assign	+,-,A,C,I,N,P	T.
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC03.4	Vendor Assignment	+,-,A,C,I,N,P	T
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC03.5	Asset Assignment	+,-,A,C,I,N,P	'l'
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC03.6	Equipment Assignm	+,-,A,C,I,N,P	T
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC03.7	Role Assignment	+,-,A,C,D,I,N	Ч
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC03.8	Roles	+,-,A,C,I	T
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC03.9	Resource Account	C,I	T.
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC04.1	GL Code	+,-,A,C,I	T
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC05.1	Account Categories	NO FC	Ч
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC06.1	Override Account Ca	+,-,C,I,N,P	'ALL_ACCESS'
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC06.2	Override Mass Add/	A,C,I	Ψ.,

🛃 Sort Ascending
ᠯ Sort Descending
<mark>∲</mark> × Remove Sort
Group By this column
Remove from groups
Show rows where:
contains 🔹
contains
And
And

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 – Security Class - Form.

$- \rightarrow G \oplus esbussness$	v9090/KK_LS9ReportingPortal/filters.htm?SE	RVERID=LSF_PROD&P	ROFILE=APS&ID=141					ର 🕁 🚺
Apps 📐 Kinsey Portal								Other bookma
	Role - Security Class - Fo	orm				<b>*</b>		Search Crite
							<u>5110W</u>	Search Chie
Expand Groups	Collapse Groups Clear Filters	Show/Hide	Columns					5,545 reco
Drag a column and	drop it here to group by that colu	mn						
Role	▲ Y Role Description Y	Security Class	Y Security Class Descript	Form	Y Form Description	Y Available FC	Y Rule	
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC00.2	Calendar	A,C,D,I,N,P	var zz=new mkUsrDat	eObj(user.getA
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC00.1	Activity Group	A,C,D,I,N,P	'I,N,P'	
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC03.2	AC Person Assignme	+,-,A,C,I,N,P	Т	
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC03.3	HR Employee Assign	+,-,A,C,I,N,P	'l'	
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC03.4	Vendor Assignment	+,-,A,C,I,N,P	'I'	
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC03.5	Asset Assignment	+,-,A,C,I,N,P	Υ	
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC03.6	Equipment Assignm	+,-,A,C,I,N,P	Ψ	
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC03.7	Role Assignment	+,-,A,C,D,I,N,P	T	
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC03.8	Roles	+,-,A,C,I	Т	
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC03.9	Resource Account	C,I	T	
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC04.1	GL Code	+,-,A,C,I	Ψ.	
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC05.1	Account Categories	NO FC	Υ	
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC06.1	Override Account Ca	+,-,C,I,N,P	'ALL_ACCESS'	
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC06.2	Override Mass Add/	A,C,I	T	
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC07.1	Account Assignment	+,-,A,C,I,N,P	var zz=new mkUsrDat	eObj(user.getA
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC08.1	Category Structure	+,-,A,C,I,N,P,X	Ч	
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC08.2	Define Category Stru	A,C,D,I,N,P	Ψ.	
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC10.1	Activity	A,C,D,I,N,P	'ALL_ACCESS'	
ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC10.2	Location Assignment	A,C,D,I,N,P	'ALL_ACCESS'	

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	Y Role Description	Y Security Class	Y Security Class DescriptY	Form Y	Form Description	Y Available FC Y	Rule

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.



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.

	Role	Y	Role Description	Υ	Security Class	Y	Security Class Descript	Form	Y	Form Description	Y	Available FC	Υ	Rule
▶	Form: CU01.1 (12)													
⊧	Form: AC00.1 (12)													
⊧	Form: AC00.2 (12)													
▶	Form: AC02.1 (8)													
•	Form: AC03.1 (8)													
	ACAccountant		ACAcc Description th		ACAnalysis		Activity Managemen	AC03.1		Resource		A,C,D,I,N,P		T.
	ACAccountant		ACAcc Description th		ACDataEntry		Activity Managemen	AC03.1		Resource		A,C,D,I,N,P		Т
	ACAssetClerk				ACAnalysis		Activity Managemen	AC03.1		Resource		A,C,D,I,N,P		T.
	ACDataEntry				ACAnalysis		Activity Managemen	AC03.1		Resource		A,C,D,I,N,P		Т
	ACExpert				ACResource		AC Resources, Roles,	AC03.1		Resource		A,C,D,I,N,P		'ALL_AC
	FinSup				ACAnalysis		Activity Managemen	AC03.1		Resource		A,C,D,I,N,P		Т
	FinSup				ACDataEntry		Activity Managemen	AC03.1		Resource		A,C,D,I,N,P		T.
	ONLYACDataEntry		ONLY ACDataEntry C		ACDataEntry		Activity Managemen	AC03.1		Resource		A,C,D,I,N,P		Т
⊧	Form: AC03.2 (8)													
•	Form: AC03.3 (8)													

The grid now displays the Roles, Security Classes 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 Security Class to the Group.

orr	n ×	– Security Class 🗙							
		Role Y	Role Description Y	Security Class	Security Class Descript	Form Y	Form Description	Available FC	YRul
►	Forn	<b>m:</b> CU01.1 (4)							
Þ	Forn	m: AC00.1 (3)							
٣	Forn	m: AC00.2 (3)							
	-	Security Class: ACAnalysis (	4)						
		ACAccountant	ACAcc Description th	ACAnalysis	Activity Managemen	AC00.2	Calendar	A,C,D,I,N,P	var
		ACAssetClerk		ACAnalysis	Activity Managemen	AC00.2	Calendar	A,C,D,I,N,P	var
		ACDataEntry		ACAnalysis	Activity Managemen	AC00.2	Calendar	A,C,D,I,N,P	vai
		FinSup		ACAnalysis	Activity Managemen	AC00.2	Calendar	A,C,D,I,N,P	var
	►	Security Class: ACDataEntry	(3)						
	►	Security Class: ACSetup (5)							
Þ	Forn	m: AC02.1 (3)							
Þ	Forn	<b>m:</b> AC03.1 (3)							

As you can see the system will now report on the number of Security Classes the Form can be found in and the number of Roles assigned to the Security Class. 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 × Sec	curity Class 🗙

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 dro	Orag a column and drop it here to group by that column									
Role	Y Security Class	Y Security Class Descript	Form	▲ Y Form Description	Y Available FC Y	Rule	Y			
ACAssetClerk	ACAnalysis	Activity Managemen	AC00.1	Activity Group	A,C,D,I,N,P	'I,N,P'	L			
ACAccountant	ACAnalysis	Activity Managemen	AC00.1	Activity Group	A,C,D,I,N,P	'I,N,P'				
FinSup	ACAnalysis	Activity Managemen	AC00.1	Activity Group	A,C,D,I,N,P	'I,N,P'				
FinSup	ACDataEntry	Activity Managemen	AC00.1	Activity Group	A,C,D,I,N,P	Ч				
ONLYACDataEntry	ACDataEntry	Activity Managemen	AC00.1	Activity Group	A,C,D,I,N,P	Ч				
ACAssetManager	ACSetup	Activity Managemen	AC00.1	Activity Group	A,C,D,I,N,P	'I,N,P,A'				
FinSup	ACSetup	Activity Managemen	AC00.1	Activity Group	A,C,D,I,N,P	'I,N,P,A'				
ACAccountant	ACSetup	Activity Managemen	AC00.1	Activity Group	A,C,D,I,N,P	'I,N,P,A'				
ACDataEntry	ACAnalysis	Activity Managemen	AC00.1	Activity Group	A,C,D,I,N,P	'I,N,P'				

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

2 Sort Ascending
🛃 Sort Descending
<b>∲</b> × Remove Sort
Group By this column
Remove from groups

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

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



#### Saving Reports

#### Saving New 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 set prior to saving the report.* 

📕 Save Repo	rt 🗶
Report Name: Report Descriptic	[] on:
	Save Report

#### **Changing and Saving an Existing Report**

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 the Overwrite existing option. To create a new report from a copy of an existing report select the New option and enter a new report name.

🖌 Save Repo	ort	×
Overwrite: 🖲 N	lew: O	
Report Name: Report Descriptio	User Role Form Report	
		/;
	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 - (6		Data Review View	Developer Add-Ins			0 -	
2		Α	В	С	D	E	F	G	
	1	Role	Role Description	Security Class	Class Description	Token	Title	Rule	
	327	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'	
	2283	AMEN	AMEN	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'	
	2609	PA	PA	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'	
	2935	PAYROLL	PAYROLL	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'	
	3261	HR	HR	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'	
	3587	HRUSER	HRUSER	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'	
	3913	ACCT-CB	ACCT-CB	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'	
	4239	WEB	WEB	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'	
	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'	
	5217	AP	AP	ActivityManagem1	[AC] System Code Tokens, Categories, Programs	ACVW.1	Build GL Accounting Unit View	'ALL_ACCESS'	
	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'	
	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 Security Class (Tasks). The following drill assignments are available.

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

To execute a drill click 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 Security Class assigned to HRGeneralist or the Users that have been assigned the HRGeneralist Role.

Drag a column and drop i	t here to group by tha	t column					
Role	Y Security Class	Security Class Descript	Form 🔺 🍸	Form Description	Available FC Y	Rule	Y
HRClerical	HRSetupInq	Inquiry only access t	HR00.1	Company	A,C,D,I,N,P	'I,N,P'	
HRDirector	HRSetup	All Access to HR Setu	HR00.1	Company	A,C,D,I,N,P	'ALL_ACCESS'	
HRClerical	HRSetup	All Access to HR Setu	HR00.1	Company	A,C,D,I,N,P	'ALL_ACCESS'	
HRGeneralist	UBCotup	All Access to HR Setu	HR00.1	Company	A,C,D,I,N,P	'ALL_ACCESS'	
HRClerica Role   Secu	blng	Inquiry only access t	HR00.2	Canada Payroll Acco	+,-,A,C,I	'I,N,P,+,-'	
HRClerica User   Role		All Access to HR Setu	HR00.2	Canada Payroll Acco	+,-,A,C,I	'ALL_ACCESS'	
HRDirecto	ппоетар	All Access to HR Setu	HR00.2	Canada Payroll Acco	+,-,A,C,I	'ALL_ACCESS'	

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

Drag a column and	drop it l	here to group by tha	t colui	mn			
Role	Y	Role Description	Y	Security Class	Y	Security Class Description	Y
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 Security Class to see the Forms and their rules assigned to the Task.

Drag a column and d	lrop it ł	nere to group by that colur	mn						
Security Class	Y	Security Class Descript¥	Form	Y	Form Description	r  .	Available FC Y	Rule	YA
HRSetup		All Access to HR Setu	HR30.2		Base Currency		C,I	'ALL_ACCESS'	
HRSetup		All Access to HR Setu	HR86.6		Test Source		A,C,D,I,N,P	'ALL_ACCESS'	
HRSetup		All Access to HR Setu	HR65.1		Human Resource Wr		A,C,D,I,N,P	'ALL_ACCESS'	
HRSetup		All Access to HR Setu	HR88.4		Human Resource Co		A,C,D,I,N,P	'ALL_ACCESS'	
HRSetup		All Access to HR Setu	HR86.8		Test User Field 3		A,C,D,I,N,P	'ALL_ACCESS'	
HRSetup		All Access to HR Setu	HR18.3		State Reporting Info		A,C,D,I	'ALL_ACCESS'	
HRSetup		All Access to HR Setu	HR65.7		Human Resource Wr		+,-,C,I,N,P	'ALL_ACCESS'	
HRSetup		All Access to HR Setu	HR81.4		Competency		A,C,D,I,N,P	'ALL_ACCESS'	
HRSetup		All Access to HR Setu	HR18.2		State Reporting Info		A,C,D,I	'ALL_ACCESS'	
HRSetup		All Access to HR Setu	HR81.5		Competency and Ce		A,C,D,I,N,P	'ALL_ACCESS'	
HRSetup		All Access to HR Setu	HR84.1		Position Reason Code		A,C,D,I,N,P	'ALL_ACCESS'	
HRSetup		All Access to HR Setu	HR84.8		Supervisor User Fiel		A,C,D,I,N,P	'ALL_ACCESS'	
HRSetup		All Access to HR Setu	HR18.4		State Reporting Info		A,C,D,I	'ALL_ACCESS'	

Alternatively you can also drill up the security tree. If you start with the Security Class -Form query you can drill up to the Roles assigned to a Security Class and continue to drill up to the Users assigned to a Role. For example let's look at the Role – Security Class 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 it here to group by that co	lumn	
Role	Y Security Class	Y Security Class Description	Y
ACAssetClerk	ACSetup	Activity Management Setup	
ACAssetClerk	ACTransaction	Activity Management Transaction Entry, Posting	
ACAssetClerk	AMProcessing	Asset Management Processing	
ACAssetClerk	AMSetup	Asset Management Setup	
ACAssetClerk	PRFiles	PR Files	
ACAssetManagor		Activity Management Setup	
ACAssetMana	AssetManager Role   Security Class		
ACBRIobSched	Jser   Role eduler	AC and Br Job Scheduler Jobs	
ACBRJobSchedurer	DataAreaAccess		
ACDataEntry	ACAnalysis	Activity Management Analysist	
ACDataEntry	ACBalanceRptInq	Activity Management Balance Reports, Inquiries	
ACDataEntry	DataAreaAccess		
ACExpert	ACAllocations	Activity Management Allocation Processing	
ACExpert	ACBalanceRptInq	Activity Management Balance Reports, Inquiries	

The User| Role option will display a list of the User's assigned to this Role.

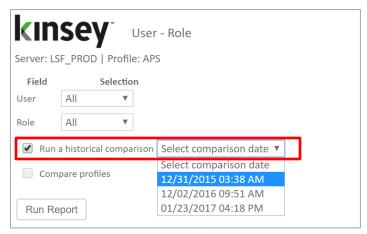
Drag a column and	l dro	op it here to group by th	nat	column			
User	Y	Full Name	Y	Role	Y	Role Description	Y
bthomas		Thomas, Bill		ACAssetManager			
schristian		Christian, Sammy		ACAssetManager			

#### **Historical Reports & Comparisons**

Historical Reports support all of the functionality found in the standard reports. You can either chose to run historical reports by selecting the appropriate Snapshot and Profile in the top right corner of the screen or you can compare your current security settings to a prior snapshot. To run historical reports select "Shapshot" from the server dropdown and choose the appropriate timestamp and profile.

Snapshot - Production - LS3SERVER V	12/04/2015 04:37 PM ▼ Select Profile ▼	h	?	(↔
	Data Last Updated:	12/04/2	2015 04:	:37 PM

To compare your security to a snapshot, first select the server and profile of your active security model in the top right corner. Then once you chose a report you will have the option to select a Snapshot for the comparison.



For more information on how to create Historical snapshots refer to the Kinsey Administrator Guide, page 12, Schedule Tasks.

#### **Comparing Profiles**

The profile comparison option allows you to compare 2 profile on the same server or cross servers. This option only uses your current security and is not available for historical comparisons.

To compare 2 profiles, first select a server and profile in the top right corner of the screen. Once you chose a report you will have the option to select the server and profile you would like use for the comparison. You have the option of comparing 2 different profiles on the same server, 2 different profiles and different servers, the same profile and different servers.

KINSEY <sup>*</sup> User - Role Server: LSF_PROD   Profile: APS	
Field     Selection       User     All       Role     All       ▼       Run a historical comparison	
Compare profiles Test - Infor 10	Select profile 🔻
	Select profile AC2
Run Report	ADM
	ASR
	ASR
	ASR CRA
	ASR CRA DV2
	ASR CRA DV2 ENV GEN GHC
	ASR CRA DV2 ENV GEN GHC KAW
	ASR CRA DV2 ENV GEN GHC

For more information on how to create Historical snapshots refer to the Kinsey Administrator Guide, page 12, Schedule Tasks.

#### **Scheduling Security 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 on the saved reports page you can click on the report name and select **Schedule Report.** 

← → C Ph esbussry:9090	0/KK_LS9ReportingPortal/filters.htm	n?SERVERID=LSF_PROD&PROFILE	=APS&ID=0				<b>Q</b> ☆
Apps 🗼 Kinsey Portal							C Other bookm
<b>kinsey</b> <sup>®</sup>	User-Defined Repo	rts				*	A ? G
Server: LSF_PROD   Pr	ofile: APS					<u>S</u>	how Search Criter
Expand Groups	Collapse Groups Clear F	Filters Show/Hide Colu	nns				12 recor
Drag a column and dr	op it here to group by tha	t column					
HIDDEN##Profile	Y Report Category	Y Report Name	Y Report Description	Y Using Report	Modified by	Y Modify date	Ƴ SchecƳ
APS	Users	TX Only	ТХ	User - Role - Task	admin	12/16/14 4:30 PM	
APS	Roles	AM Hist	al Report	Role - Task - Form	admin	4/30/15 9:24 AM	
APS	Users	Finance Run Repo		User - Role - Task - F	admin	6/19/15 12:55 PM	0
APS	Roles	Manage Schedule	-	Role - Task	admin	9/29/15 10:05 AM	0
APS	Tasks	Acbudge <u>Delete</u>		Task - Form	admin	9/29/15 11:11 AM	(1)
APS	Roles	All Roles Except xyz		Role - Task	admin	10/26/15 2:15 PM	
APS	Users	Finance User Role R		User - Role	admin	11/5/15 11:16 AM	0

A grey clock icon is displayed at the end of the line if a schedule already exist for a report but has not been 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</li> <li>Create new schedule</li> <li>Every Morning</li> <li>04</li> <li>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.

Email format:

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**

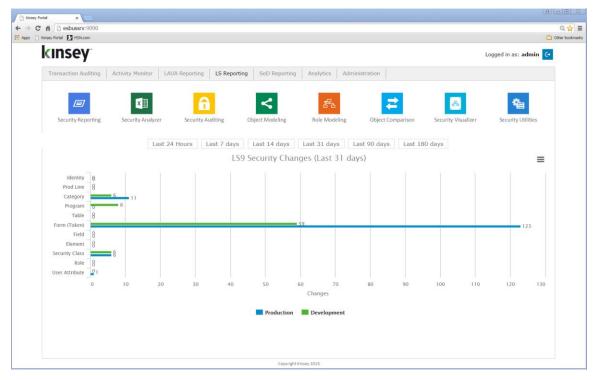
To delete a report, select the report name and click on Delete. You must have the proper permissions to delete a report.

#### **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 Security Classes are defined are part of the Security Reports describe in the prior section of this manual

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.

← → C f Cesbussrv:9090/LS9_Report/			@ ☆ ≡
🔛 Apps 🔱 Kinsey ESBus Home Pa 🚺 MSN.com			Cther bookmarks
kinsey <sup>*</sup> 📧 Security Analyzer			â ? C+
Lawson Server Selection Select Server Select Server http://ls3server.corpnet.lawson.com http://ls3server.corpnet.lawson.com	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.



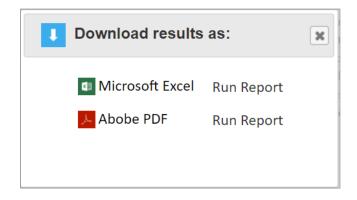
The page will then allow you to select Roles and Users for building your selection criteria. The purpose of the Role filter is to create a list of users that have been assigned to a selected Role. This is NOT an indication of the Roles that will print on the report. Every Role for every selected User will be included on the report. As user's are added and removed from the selected roles the user list will change. The alternative is to select the User's manually. This list will be static and not based on the role criteria.

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

→ C (i) esbussrv:9090	// S9 Report/			० 🕁 🗖
Apps Kinsey Portal	hes_mpony			Cther book
(Insey	Security Analyzer			🖳 🚔 ? 🤇
	Infor Server Selection Production - LS3SERVER	Infor Profile  * APS	6/9/2017 1 ✔ Only show users with identity: LSF901	1:33AM
	Saved Reports	Roles (with tasks attached)	Users (with roles attached)	
	AC Only	ACAccountant	adavis (Davis, Angie)	
		ACAsceduntant	w awhite (White, Al)	
		ACAssetManager	✓ bthomas (Thomas, Bill)	
	All	🖍 😝 🛛 🖉 ACBRJobScheduler	fnelson (Nelson, Frank)	
	BR Roles	ACDataEntry	hroberts (Roberts, Helen)	
	BThomas	ACDataEntry	Interest (Rogers, Hal)	
	Financial Users	APInquery	<ul> <li>isolatedsoduser (SOD, Isolated)</li> <li>lawson (Lawson, Lawson)</li> </ul>	
	fnelson	AFriduely APSetupInquiry	<ul> <li>Iawson (Lawson)</li> <li>mnitka (Nitka, Mike)</li> </ul>	
		✓ 🙂 🖉 ARSuper	Schristian (Christian, Sammy)	
		✓ 🕃 🛛 🖉 AllAccessRole	✓ smiller (Miller, Sarah)	
		🖌 😝 🛛 ApplicantRole		
	Roberts Miller	BRBiller		
	schristian			
	Super Users	BRExpert		
			*	
		Report Name		
		Query Description		
				h
		SAVE CANCEL		

#### **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. 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.



Select your preferred 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.

#### 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.



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

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

#### **Users Assigned Roles**

-	19-01-	] <mark>(2</mark> ∰ 2 ♥ ∰ <b>(</b> 2) =						380363195.xisx - Mic	rosoft Excel							
H	ome Inser	Page Layout Formulas	Data Rev	new View	Developer Add-Ins											
	Cut	Calibri - 10 - A	A = =		Wrap Text Gene	ral =		Normal	Bad	Good	Neutral	Calculation	📑 📴 🏞	Σ AutoSum · A	8	
	Copy	B Z U - H - 3- A	- = = :	-	Merge & Center - S -	16 . 28 .28	Conditional	Format Check Cell	Explanatory	Input	Linked Cell	Note	Insert Delete	Fill - Sort	k Find &	
Club	Format Painte	Font		Alignmer		Number 5	Formatting *	is Table +		h fire			Cells		* Select *	
			- 21	Andhumkt		Number 3				t) fes			Cent	cound		
11	121-1-1-1		1 12	1 2	1 2	1 22			-	10	- 12	-		1111		
	A B	C	D	E	F	G		н		1	1		К.	i ka	M	
1 5	Summary of La	wson Access (LS9 Security) - Form	s			ACAssetClerk							Roles assigned to User			
						WHTK18050Files										
						ProcessFlowRole										
						ACAccountant										
						HR7T16095(Files										
						GLReportWritter										
						HRGeneralist										
						GLAccountant										
						APSuper										
						GLSuper										
						POBuyer ACDateEntry										
						HRDirector										
						ACExpert										
						rNewRole										
						APInquery										
						AllAccessRole					ACAssetClerk					
						ACAssetManager					SODGL40Update					
						HRClerical					ACDataEntry					
						PortalBookmark/	dminRole				rSecLevelOS			FormPersonalizationRole		
						EFSAdmin					ACExpert			PortalBookmarkAdminRole		
						BatchRole					SuperAdminRole			ProcessFlowRole	ACAssetManager	
						ACBRJobSchedule	r				ACAccountant			EFSAdmin	GLACCT48	
						ManagerRole					FinSup			SuperAdminRole	GLACCT5CB	
						SuperAdminRole					AllAccessRole			BatchRole	APInquery	
						LawsonQueryToo		PortalBookmarkAdminRole			ARSuper			LawsonQueryToolsRole	APSuper	
2 (	no descriptio	n)				ARSuper		BatchRole	SuperAdminRo	ole	APSuper	Proc	essFlowRole	AllAccessRole	GLAccountant	
3	iys .												Users			
	Code Form I	Title	Role	Security Class	Available Functions	smiller		Isuser	Isadm		mnitka	pfad	min	hroberts	fnelson	
5 4	AC ACOD 1	Activity Group			A,C,D,I,N,P	ALL_ACCESS		NO ACCESS	NO ACCESS		ALL_ACCESS	NO A	CCESS	NO ACCESS	NO ACCESS	
10 4	AC ACOD.2	Calendar			A,C,D,I,N,P	ALL_ACCESS		NO ACCESS	NO ACCESS		ALL_ACCESS	NO A	CCESS	NO ACCESS	NO ACCESS	
15 A	AC ACOD 3	Activity Group Purge Status			C,I,N,P	ALL_ACCESS		NO ACCESS	NO ACCESS		ALL_ACCESS	NO A	CCESS	ND ACCESS	NO ACCESS	
18 4	AC ACOL1	Mass Activity Copy			+-ACD.F.I.M.N.P.R.U.V.			NO ACCESS	NO ACCESS		ALL ACCESS	NO A	CCESS	NO ACCESS	NO ACCESS	
20 A		Additional Parameters			NO FC	ALL_ACCESS		NO ACCESS	NO ACCESS		ALL_ACCESS	NO A	CCESS	NO ACCESS	NO ACCESS	
22 4		Inquire Filter			NO FC	ALL_ACCESS		NO ACCESS	NO ACCESS		ALL_ACCESS		CCESS	NO ACCESS	NO ACCESS	
		Automatic Activity			A.C.D.I	ALL ACCESS		NO ACCESS	NO ACCESS		ALL ACCESS	NO A		NO ACCESS	NO ACCESS	

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 (TKN)

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 classes.

<b>C.</b>		<b>17</b> - (1	1 - Lì 🖆	• 🖨 🛕 🖤 😰 ) =				380363195.xl	x - Microsoft Excel		
<b>(C</b> )	н	ome	Insert	Page Layout Formulas Data	Review Vie	w Developer	Add-Ins				
Norr	nal Pa Lay	out Pr	e Break O	stom Full lews Screen Show/Hide	4	m 100% Zoom to Selection Zoom	New Arrange Freeze	Split         ① View Side by Side           Hide         :a1 Synchronous Scrolling           Unhide         :e3 Reset Window Position           Window         Window	Save Switch Macros		
1148 • A NO ACCESS											
1 2		А	В	С	D	E	F	G	Н	L. L.	J
	4	Sys Code	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
+	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
+	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	Α	NO ACCESS	NO ACCESS	A,I
+	32	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	-	AC03.3	HR Employee Assignment			+,-,A,C,I,N,P	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS
+	44	AC	AC03.4	Vendor Assignment			+,-,A,C,I,N,P	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS
+	48	AC	AC03.5	Asset Assignment			+,-,A,C,I,N,P	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS
+	52	AC	AC03.6	Equipment Assignment			+,-,A,C,I,N,P	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.* 

						380363195	.xlsx - Mic	rosoft Exc	el			Settings			? ×
Data Review	w View	Developer Add-Ir	15									Direction			
Connections Properties Con Section	$ \begin{array}{c} \underline{A} \downarrow \\ \underline{Z} \downarrow \\ \underline{Z} \downarrow \\ \underline{A} \downarrow \\ \end{array} $ Sort	Filter	Text to Remov Columns Duplica	e Data	Consolidate	What-If Analysis *	Group	Ungroup	333	<ul> <li>Show Det</li> <li>Hide Deta</li> </ul>		Summary row	umns to right of d	etail	
Connections	nections Sort & Filter			Data Tools			Outline			5					
										_		Create	Apply Styles	ОК	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	Α	В	С	D	E	F	G	Н	I.	J
			iys Iode	Form ID	Tiala	Role	Security Class	Available Functions	emiller	lauraa	landen	maitka
	4	• •	Loue	Form ID	Inte	Role	Security Class	Available Functions	smiller	lsuser	lsadm	mnitka
-	93	3 4	AC	AC10.1	Activity			A,C,D,I,N,P	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS
	• 94	4 A	AC	AC10.1	Activity	ACAccountant	ACSetup	A,C,D,I,N,P	ALL_ACCESS			ALL_ACCESS
	• 9	5 4	AC	AC10.1	Activity	ACAssetManager	ACCapitalization	A,C,D,I,N,P	ALL_ACCESS			
	• 9	6 A	AC	AC10.1	Activity	ACExpert	ACCapitalization	A,C,D,I,N,P	ALL_ACCESS			ALL_ACCESS
	• 9	7 4	AC	AC10.1	Activity	ACExpert	ACSetup	A,C,D,I,N,P	ALL_ACCESS			ALL_ACCESS
	• 9	8 4	AC	AC10.1	Activity	FinSup	ACAnalysis	A,C,D,I,N,P				I
IL	• 9	9 4	AC	AC10.1	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.

<b>9</b>	J	🗋 💕 🖨				380363195.xtsx - Microsoft Excel			
	Home Insert Page Layout Formulas Data Review View Developer Add-Ins								
	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									

Additional sheets exist for the following objects:

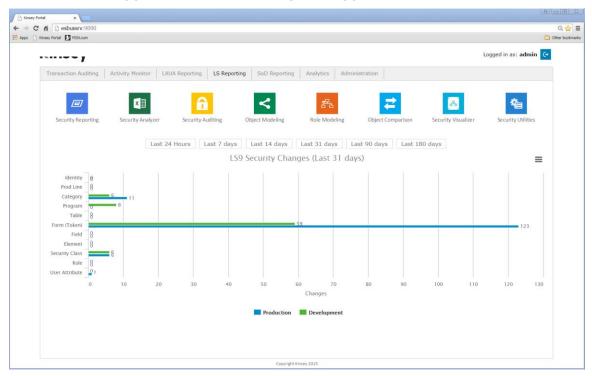
٠	CAT	Categories
•	DTL	Detail Pains
•	ELG	Element Groups
•	ELS Conditions	Element Group Conditions
•	ELM	Elements
•	FLD	Fields
•	FLC Conditions	Field Conditions
•	HDN	Hidden Fields
•	PDL	Product Lines
•	PGM	Program Codes
•	RMO	Resource Manager Objects
•	RPT	Reports
•	TBL	Tables

- TBL Conditions Table Conditions
- TFL Table Fields
- TKN Tokens (Forms)
- TKN Conditions
   Token Conditions
- TYP Securable Types

# **Change Audit Reporting**

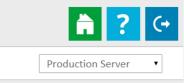
The Change Audit Report builder provides a streamlined approach tracking all changes made to your Lawson Security model. This flexible report writer allows you to track the security changes most important to you and setup automatic email notifications.

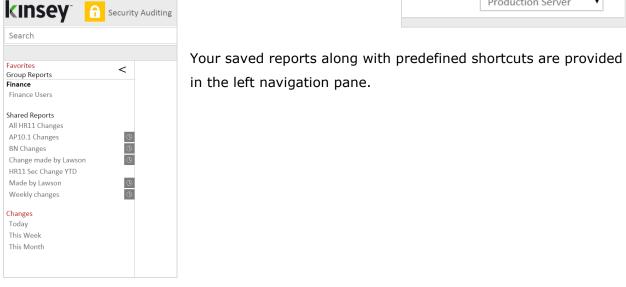
*Note: Lawson Security Auditing must be enabled in the Lawson Security Administrator application before using this application.* 



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.



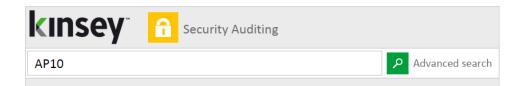


🗅 Kinsey Security Auditing 🛛 🗙 📃			
	- 01	RVERID=LSF_PROD&QUERY=ap10&_nq=1&_s=1	Q 😒
Apps 🚺 Kinsey ESBus Home Pa 🚺 MSN.ci	om		C Other bookma
kinsey 🔂	Security Au	diting	💵 ≽ 🖬 🗣 🚔 ? 😔
ap10		Advanced search	roduction Server • Results per page: 25 •
		Action Date/Time User Affects Profile Role Security C	lass Type Object Previous Rule Current Rule
Favorites Group Reports	<	🏓 D-Delete 11/23/201411:23 PM lawson - DPS - APSetup01a TKN AP10.8	ALL_ACCESS' - 🛛 🕵 人
Finance		🏓 U - Update 11/23/2014 11:23 PM lawson - DPS - APSetup01a TKN AP10.8 '	ALL_ACCESS' 'ALL_ACCESS' 💷 人
Finance Users		🏕 A - Add 11/23/2014 11:23 PM lawson - DPS - APSetup01a TKN AP10.6 -	'ALL_ACCESS' 💶 ≽
Shared Reports		衫 A - Add 11/23/2014 11:23 PM lawson - DPS - APSetup01a TKN AP10.7 -	'ALL_ACCESS' 💶 ≽
All HR11 Changes AP10.1 Changes	<b>()</b>	🎶 A - Add 11/23/2014 11:23 PM lawson - DPS - APSetup01a TKN AP10.4 -	'ALL_ACCESS' 💶 人
BN Changes	(3)	🏓 A - Add 11/23/2014 11:23 PM lawson - DPS - APSetup01a TKN AP10.5 -	'ALL_ACCESS' 💶 人
Change made by Lawson HR11 Sec Change YTD	0	🏓 A - Add 11/23/2014 11:23 PM lawson - DPS - APSetup01a TKN AP10.2 -	'ALL_ACCESS'
0	3	A - Add 11/23/2014 11:23 PM lawson - DPS - APSetup01a TKN AP10.3 -	'ALL_ACCESS' 💷 人
Weekly changes	0	A - Add 11/23/2014 11:23 PM lawson - DPS - APSetup01a TKN AP10.1 -	
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 -	
This Week This Month			
		Previous 1 Next	
		Page 1 of 1 pages (0.19 seconds)	
	<i>l</i> i	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.

Prompt at runtime:	Search Criteria:	Column Name:
	▼ AP10	Any Field    Contains
Prompt at runtime:	Search Criteria:     Beginning of Month      Current Date	Column Name: Audit Date/Time • ] [between
Prompt at runtime:	Search Criteria:	Column Name: Not Selected • Not Selected
Prompt at runtime:	Search Criteria:	Column Name: Not Selected • Not Selected
Prompt at runtime:	Search Criteria: ▼	Column Name: 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 <b>T</b>	
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.

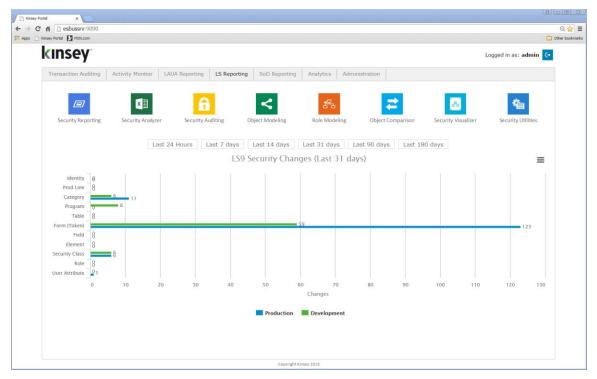
#### **Renaming a Report**

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 ▼	ĥ	?	ۥ
	Data Last l	Jpdated: :	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	
<ul> <li>✓</li> </ul>	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 P	fortal ×	) Kinsey Portal × 🗅 Kinsey Object Modeling	×							Ağı e X
		0090/KK_LS9ReportingPortal/what-If.htm?SE	RVERID=LSF_PROD&PROF	ILE=APS						@ ☆ ≡
👯 Apps 🚦	Kinsey ESBus Home Pa	MSN.com								C Other bookmarks
kır	<b>isey</b> <sup>®</sup>	Cbject Modeling					Production Se	rver • * A	APS •	? ↔
									Data Last Updated	: 12/3/14 14:43
Search	AP10.1					Object Rel	ationships			
Tuno	5.u	stem Code Name Description	# of SoD Rules			Us	er - smiller	<u>Hide</u>		
Type	xecutable AP		2							
Form/E	xecutable AP	AP10.1 Vendor	2	Run SOI	O Report					
The state										
Find	Affected Obje	cts								
										_
Status	Task		Task Rule		Role		User		Rule	
	VSS	Vendor Self Service	I.N.P		FinSup -		hrogers	Rogers, Hal	ALL_ACCESS	
	MNitkaAdmin		P.N.I		GLAccountant -	-	-	Nitka, Mike	-	
					VendorRole -				ALL_INQUIRES	
l 🔨	APSetup	Accounts Payable Setup Screens	A,C,D,I,N,P 🔐		vendorkole -		smiller	willer, Sarah	ALL_INQUIRES	
<ul> <li>✓</li> </ul>	Controller	Controller	1							
<b>V</b>	zzAPInquiry	zzAPInquiry	ALL_INQUIRES	1						
		Add object to a Task								
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 start of the start of</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

🗈 Kinsey Portal X 🕐 Kinsey Portal X	
← → C n	@☆ ≣
🔛 Apps 🛐 Grany (58)ua Home Pa 🚺 HSI.com	Cther bookmarks
kinsey Sobject Modeling	? (+
- Data Last Updated:	12/3/14 14:43
Search AP10.1     Object Relationships       Type     System Code     Name     Description     # of SoD Rules       Form/Executable     AP     AP10.1     Vendor     2	
Find Affected Objects	_
Status Task Task Rule Role User Rule	
VSS Vendor Self Service I,N,P / FinSup - hrogers Rogers, Hal I	
MilitkaAdmin P.N.I GLAccountant - mnitka Nitka, Mike I	
APSetup Accounts Payable Setup Screens A.G.D.I.N.P VendorRole - smiller Miller, Sarah ALL_INQUIRES	
Controller Controller	
✓ zzAPInquiry zzAPInquiry ALL_INQUIRES	
Add object to a Task	
Change Log Disabled security class: APSetup Copyright (c) 2015	

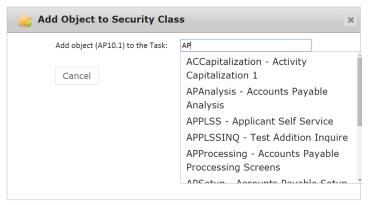
Anytime a users access level changes the new rule will turn to the color orange. To see why the user has this rule click on the user ID. The application will map the user to their available Tasks. In the example below the user *mnitka* also had access to AP10.1 through

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	lortal x	C Kinsey Portal	×) 🗈 K	insey Object Modeling	×									
	🕈 🏦 🗋 esbussrv		portingPortal/	what-if.htm?SER	VERID=LSF_PRO	D&PROF	ILE=APS							© ☆ 🗉
👯 Apps 🔱	Kinsey ESBus Home Pa	MSN.com												Cther bookmarks
kır	<b>isey</b>	< 0	Object M	odeling						Prod	luction Se	rver • * A	.PS •	? (~
													Data Last Update	ed: 12/3/14 14:43
Search	AP10.1								Object Re	elation	ships			
Туре	5	ystem Code	Namo	Description	# of SoD R	uloc				Task - /	APSetup	<u>Hide</u>		
	xecutable A		AP10.1		# 01 30D K	ules	D	Desert		Jser - I	mnitka	<u>Hide</u>		
, .					-		Run SOE	Керогс						
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>	MNitkaAdmir	n			P,N,I			GLAccountant	-		mnitka	Nitka, Mike	1	
×	APSetup	Accounts [	Payable Se	tup Screens	A,C,D,I,N,P	<b>.</b>		VendorRole	-		smiller	Miller, Sarah	ALL_INQUIRES	
	Controller	Controller			1		/							
~	zzAPInquiry	zzAPInquir	'y		ALL_INQUI	RES								
		Add o	bject to a	Task										
Change	log													
	ed security clas	s: APSetup												
							Copyr	ight (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.

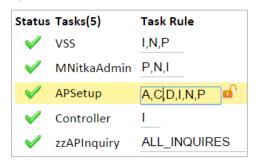
Kinsey Portal X Kinsey Portal X Kinsey Object Modeling	×			
← → C f lesbussrv:9090/KK_LS9ReportingPortal/what-if.htm?SERVE	RID=LSF_PROD&PROFILE=APS			@ ☆] ≡
🔛 Apps 🕺 Kinsey ESBus Home Pa 🚺 MSN.com				Dther bookmarks
KINSEY <sup>*</sup> < Object Modeling		Produ	ction Server • * APS	· 🔒 ? 😔
			Data	Last Updated: 12/3/14 14:43
Search         AP10.1           Type         System Code         Name         Description           Form/Executable         AP         AP10.1         Vendor           Find         Affected         Objects         A	# of SoD Rules 2 Run SOD F	Object Relations Task - AF User - m Vser - m	Setup <u>Hide</u>	
Status Task Vendor Self Service MNitkaAdmin	Task Rule I,N,P P,N,I	Role FinSup -	User hrogers Rogers, Hal mnitka Nitka, Mike	Rule I A,C,D,I,N,P
APSetup     Controller     Controller	A,C,D,I,N,P of	VendorRole - ACExpert -	smiller Miller, Sarah lawson Lawson, Lawson	ALL_INQUIRES
<ul> <li>zzAPInquiry zzAPInquiry</li> <li>ACCapitalization Activity Capitalization 1</li> <li>Add object to a Task</li> </ul>	ALL_INQUIRES A,C,D,I,N,P	ACAssetManager -		
Change Log Disabled security class: APSetup Added security class: ACCapitalization	Copyrig	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 F	rortal >	Kinsey Portal ×	Kinsey Object Modeling	×							
€ ⇒ 0	🕈 🏦 🗋 esbus	srv:9090/KK_LS9ReportingF	Portal/what-if.htm?SER	VERID=LSF_PROD&PRO	FILE=APS						© ☆ ≣
👯 Apps [	Kinsey ESBus Home Pa	MSN.com									C Other bookmarks
kı	ısey	C < Objec	t Modeling					Production S	erver • * A	APS •	? 🗘
	-									Data Last Update	d: 12/3/14 14:43
Search	AP10.1						Object Re	lationships			
Туре		System Code Nam	e Description	# of SoD Rules			Ta	ask - APSetup	<u>Hide</u>		
	xecutable		0.1 Vendor	2	Run SO	O Report					
Find	Affected Ol	hierts									
Tind	Anected of	ojecto									
Status	Task			Task Rule		Role		User		Rule	
<b>v</b>	VSS	Vendor Self Serv	/ice	I,N,P		FinSup -		hroger:	Rogers, Hal	A,C,I	
<ul> <li>Image: A start of the start of</li></ul>	MNitkaAdr	nin		P,N,I		GLAccountant -		mnitka	Nitka, Mike	A,C,I	
<b>V</b>	APSetup	Accounts Payabl	le Setup Screens	A,C,I	-	VendorRole -		smiller	Miller, Sarah	ALL_INQUIRES	
	Controller	Controller		I.							
<ul> <li>Image: A second s</li></ul>	zzAPInquir	y zzAPInquiry		ALL_INQUIRES							
		Add object	<u>to a Task</u>								
Change	-										
Change	ed security c	lass: APSetup from A	A,C,D,I,N,P to A,C	.,I							
					Сору	right (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	fortal X	🗅 Kinsey Portal 🗙 🗅 Kinsey Object Modeling	×						
		9090/KK_LS9ReportingPortal/what-if.htm?SER	/ERID=LSF_PROD&PRO	FILE=APS					० ☆ ≡
Apps 🚷	Kinsey ESBus Home Pa	MSN.com							C Other bookmarks
kır	<b>isey</b> <sup>®</sup>	Cbject Modeling				Production Se	ver • A	ps 🔹 🛱	? (+
								Data Last Updated: 1	2/3/14 14:43
Search	AP10.1								
Туре	Sy	stem Code Name Description	# of SoD Rules						
Form/E	xecutable AF	AP10.1 Vendor	2	Run SOD Repo	rt				
Find /	Affected Obje	ects							
					FinSup				
					Roles - Tasks				
Status			Task Rule	Role	<u>Role - Task - F</u>			Rule	
<ul> <li>✓</li> </ul>	VSS		I,N,P	FinSu		-	Rogers, Hal	-	
<ul> <li>✓</li> </ul>	MNitkaAdmir		P,N,I		ountant -		Nitka, Mike	-	
<ul> <li>✓</li> </ul>	APSetup	Accounts Payable Setup Screens	A,C,D,I,N,P 🔐	Vendo	orRole -	smiller	Miller, Sarah	ALL_INQUIRES	
<ul> <li>✓</li> </ul>	Controller	Controller	I.						
<ul> <li>✓</li> </ul>	zzAPInquiry	zzAPInquiry	ALL_INQUIRES						
		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

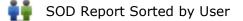
*Note: this option is only available if you have purchase the SOD application.* 

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.

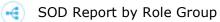
	sey "		et Mardallum									C Other bo
cins	sey	< Obje	at Mandallin a									
			ct wodeling					Pro	duction Se	rver • * A	IPS •	? (
earch AP1	10.1									Object Relat	Data Last Updated ionships	l: 12/3/14 14
ype orm/Exec	Sy sutable AP	stem Code Na AP1	me Description 10.1 Vendor	# of SoD Rules	Run SO	D Report	<b>!!</b> 🗐			Tasi	k - APSetup <u>Hide</u>	
Find Affe	ected Obje	ects							_			
tatus Tas	sk			Task Rule		Role			User		Rule	
VS:	S	Vendor Self Ser	rvice	I,N,P		FinSup	· -		hrogers	Rogers, Hal	A,C,I	
V MM	NitkaAdmin			P,N,I	_/	GLAccountant	-				A,C,I	
V AP	Setup	Accounts Payal	ble Setup Screens	A,C	1	VendorRole	-		smiller	Miller, Sarah	ALL_INQUIRES	
V Co	ntroller	Controller		T								
V zzA	APInquiry	zzAPInquiry		ALL_INQUIRES								
		Add objec	<u>t to a Task</u>									

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

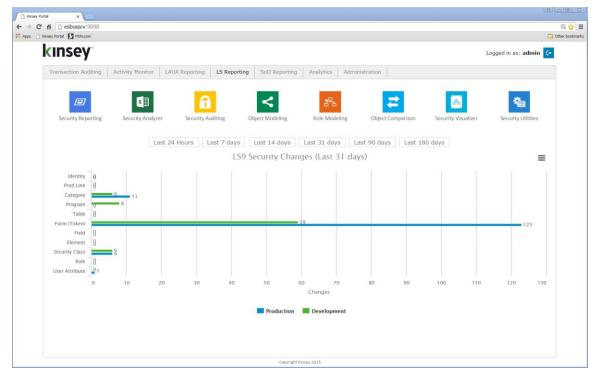




# **Role Modeling**

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 specific 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.

							▲ – □ ×
Kinsey Role Modeling X							
	.S9_Report_WhatIf/?SERVERID=LSF_P	ROD&PROFILE=APS					@☆ 🖬 :
Apps 🗶 Kinsey Portal							Other bookmarks
kinsey	器 Role Modeling			Set	t as default Production - L	S3SERVER V APS V	ስ ? ↔
						Data Last Upda	ted: 6/9/2017 11:33AM
[	Add a Role	Remove a Role	e Add a Security Class	Remove a Security Class	Run Report	Run SOD Report	No Changes
Available Users:	Co	ontains:	Add Role:	Contains:			
Select		•	Select		•		
Select adavis - Davis, Angie awhite - White, Al bthomas - Thomas, Bill frelson - Nelson, Frank hroberts - Roberts, Hel hrogers - Rogers, Hal isolatetsoduser - SOD, lawson - Lawson, Laws mitka - Nitka, Mike schristian - Christian, S smiller - Miller, Sarah	en Isolated on		I Role				
			Copyright	(c) 2017 - ver 5.0			

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 pre-saved report. For instructions on how to create a new report refer to the Securty Analzer section of this manual.

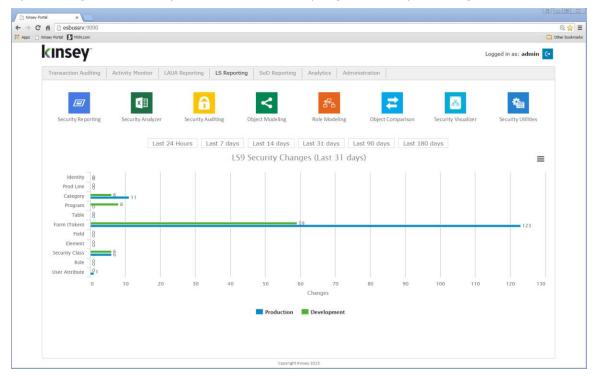
Kinsey Security Analyzer × ← → C ③ esbussry:9090/				० 🕁 🚺
Apps 📐 Kinsey Portal				📙 Other bookmar
<b>(Insey</b>	Security Analyzer			■, 🗎 ? ↔
	Infor Server Selection	Infor Profile	6/9/2017 11:33AM	
	Production - LS3SERVER	▼ * APS	<ul> <li>Only show users with identity: LSF901</li> </ul>	
	Saved Reports	<ul> <li>Roles (with tasks attached)</li> </ul>	Users (with roles attached)	
	AC Only	ACAccountant	▲ adavis (Davis, Angie)	
	ACAccountant (Nelson & Nitka)	🕑 🖉 ACAssetClerk	✓ awhite (White, Al)	
	ACBRJobBBalh	ACAssetManager	🖉 bthomas (Thomas, Bill)	
	All	ACBRJobScheduler	🖉 fnelson (Nelson, Frank)	
	BR Roles	ACDataEntry	Involve (Roberts, Helen)	
	BThomas 🗾	ACExpert	<ul> <li>hrogers (Rogers, Hal)</li> <li>isolatedsoduser (SOD, Isolated)</li> </ul>	
	Financial Users	APInquery	lawson (Lawson, Lawson)	
	fnelson 🗾	APSuper	mnitka (Nitka, Mike)	
	H Roberts	ARSuper	Schristian (Christian, Sammy)	
	HR Users	AllAccessRole	🗷 smiller (Miller, Sarah)	
	new 🗾	ApplicantRole		
	Roberts Miller	<ul> <li>Ø BRBiller</li> <li>Ø BRContractAdministrator</li> <li>Ø BRExpert</li> </ul>		
	schristian 📝	BRContractAdministrator		
	Super Users	BRReportingAdministrator		
			•	
		Report Name		
		Query Description		
				//
		SAVE CANCEL		
		Copyright (c) 20	17	

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

_	_		° 🗅 🖨 🗋 (			1390850135 - Mic	IOSOIT EXCEL			
File	G1		Insert Pag	ge Layout Formulas Data Review	View Developer	Add-Ins Acrobat				∞ 🕜 🗆 (
2		A	В	C	D	E	F	G	Н	1
	1	Summ	ary of Law	vson Access (LS9 Security) - Forms	;			Roles assigned to User		
	2	Roles a	added to u	users:Roles deleted from users:fne	lson = {ACExpert	}		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		
ы	22	AC	AC01.4	Automatic Activity			A,C,D,I	NO_ACCESS		
ы	24	AC	AC01.5	Automatic Level			A,C,D,I	NO_ACCESS		
9	26	AC	AC02.1	Status			+,-,A,C,I	L. C.		
9	30	AC	AC03.1	Resource			A,C,D,I,N,P	L. C.		
•	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	L. C.		
E	46	AC	AC03.5	Asset Assignment			+,-,A,C,I,N,P	I		
ы	50	AC	AC03.6	Equipment Assignment			+,-,A,C,I,N,P	L		
ы	54	AC	AC03.7	Role Assignment			+,-,A,C,D,I,N,P	I		
ы	58	AC	AC03.8	Roles			+,-,A,C,I	I		
ы	62	AC	AC03.9	Resource Account			C,I	I		
. [	66	AC	AC04.1	GL Code			+,-,A,C,I	I		
. [	69	AC	AC05.1	Account Categories			NO FC	I		
9	72	AC	AC06.1	Override Account Categories			+,-,C,I,N,P	I		
e (	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 ×	× Kinsey Object Comparison ×				
	esbussrv:9090/KK_LS9Re Kinsey ESBus Home Pa MSN.com	portingPortal/compare.htm?SERVERID=LS	PROD&PROFILE=APS			@☆]≡
						C Other bookmarks
КІГ	ISEY 🔁 Objec	t Comparison			Production Server   * APS	<b>A</b> ? (~
Compare	what? Roles 🔹 🔲 Compa	re objects Compare				Records: 792
⊽=	Role (a)		mmon Similarity (%) bjects		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 Copyright (c) 20:			

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.

	Bus Home Pa 🚺 MSN.	KK_LS9ReportingPortal/compare	.ntm?SERVERIL	)=LSF_PROD&PROF	ILE=APS					O,
nsey		Comparison							Production Server  * APS	• 👌 ?
re what? Role										Record
Role (a)		Role (b)		Common Similarity (9 Objects	6)			Absorbed (%)		
	conAdminRole (94)	SmartReconRole (90	)	90			95.7%			100.0%
Object Ty	pe Object	Role (a) Task	Rule	Role (b) T	ask	Rule				
CAT	AP	SmartReconAdminRole SMR	'ALL_ACCESS'	SmartReconRole Si		'ALL_ACCESS'				
CAT	CS	SmartReconAdminRole AllGENAcce	ss 'ALL_ACCESS'	SmartReconRole A	liGENAccess	'ALL_ACCESS'				
CAT	IC	SmartReconAdminRole SMR	'ALL_ACCESS'	SmartReconRole SI	MR	'ALL_ACCESS'				
CAT	IS	SmartReconAdminRole AllGENAcce	ss 'ALL_ACCESS'	SmartReconRole A	liGENAccess	ALL_ACCESS				
CAT	LO	SmartReconAdminRole Bookmark	'ALL_ACCESS'	SmartReconRole B	ookmark	'ALL_ACCESS'				
CAT	MA	SmartReconAdminRole SMR	'ALL_ACCESS'	SmartReconRole Si	MR	'ALL_ACCESS'				
CAT	PO	SmartReconAdminRole SMR	'ALL_ACCESS'	SmartReconRole Si	MR	'ALL_ACCESS'				
CAT	RD	SmartReconAdminRole Bookmark	'ALL_ACCESS'	SmartReconRole B	ookmark	'ALL_ACCESS'				
CAT	SC	SmartReconAdminRole AllGENAcce	ess 'ALL_ACCESS'	SmartReconRole A	llGENAccess	s 'ALL_ACCESS'				
CAT	UN	SmartReconAdminRole AllGENAcce	ss 'ALL_ACCESS'	SmartReconRole A	liGENAccess	s 'ALL_ACCESS'				
PDL	PDL\$_\$GEN	SmartReconAdminRole AllGENAcce	ss 'ALL_ACCESS'	SmartReconRole A	liGENAccess	s 'ALL_ACCESS'				
PDL	PDL\$_\$LIVE	SmartReconAdminRole SMR	'ALL_ACCESS'	SmartReconRole Si	MR	'ALL_ACCESS'				
PDL	PDL\$_\$LOGAN	SmartReconAdminRole Bookmark	'ALL_ACCESS'	SmartReconRole B	ookmark	'ALL_ACCESS'				
PGM	LO12	SmartReconAdminRole Bookmark	'ALL_ACCESS'	SmartReconRole B	ookmark	'ALL_ACCESS'				
PGM	LO13	SmartReconAdminRole Bookmark	'ALL_ACCESS'	SmartReconRole B		'ALL_ACCESS'				
PGM	L014	SmartReconAdminRole Bookmark	'ALL_ACCESS'	SmartReconRole B		'ALL_ACCESS'				
PGM	LO15	SmartReconAdminRole Bookmark	'ALL_ACCESS'	SmartReconRole B		'ALL_ACCESS'				
PGM	MA67	SmartReconAdminRole SMR	'ALL_ACCESS'	SmartReconRole Si		'ALL_ACCESS'				
PGM	RD69	SmartReconAdminRole Bookmark	'ALL_ACCESS'	SmartReconRole B		'ALL_ACCESS'				
PGM	UNJS	SmartReconAdminRole AllGENAcce	-	SmartReconRole A		-				
PGM	UNPD	SmartReconAdminRole AllGENAcce	-	SmartReconRole A		-				
PGM RMO	UNPM	SmartReconAdminRole AllGENAcce SmartReconAdminRole AllRMAcce	-	SmartReconRole A	IGENACCES	ALL_ACCESS				
RMO	Group	SmartReconAdminRole AllRMAcce SmartReconAdminRole AllRMAcce	-							
RMO	Resource Role	SmartReconAdminRole AllRMAcce	-			-				
NIVIO	Structure	SmartReconAdminRole AllRMAcce	-							

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.

Iľ	isey 🔁	Object Compa	rison			Production Server   MJN	• other ba
par	e what? Tasks 🔹 🗌	Compare rules	Compare				Records: 2
⊽=	Task (a)	Task (b) =	Common Objects	Similarity (%)		Absorbed (%)	
+	AMUpdates01 (2)	AMUpdates02 (2)	) 2		100.0%		100.0%
-	AMUpdates02 (2)	AMUpdates01 (2)	) 2		100.0%		100.0%
	Object Type Object CAT AM	Task (a) AMUpdates02	-	Task (b) Rule AMUpdates01 'ALL_ACCES			
	TKN AM145	AMUpdates02	'ALL_ACCESS'	AMUpdates01 'I,J,M,N,P,R'			
+	HRSetup03 (2)	HRSetup04 <mark>(</mark> 3)	2		66.7%		66.7%
+	HRSetup04 <mark>(</mark> 3)	HRSetup03 (2)	2		66.7%		100.0%
+	IFSetup00 (141)	IFSetup01 (73)	73		51.8%		100.0%
+	IFSetup01 (73)	IFSetup00 (141)	73		51.8%		51.8%
+	APSetup00 (90)	APSetup01 (42)	42		46.7%		100.0%
L.			12		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.

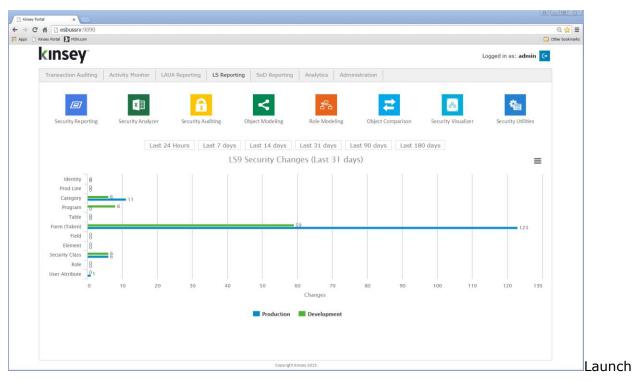
C Kinsey P → C	ortal × C Kinsey Portal	× 🗈 Kinsey Object Compa		ROD&PROFILE=APS			
Apps <u>8</u>	Kinsey ESBus Home Pa 🚺 MSN.com						Cther bookma
<b>(I</b> ľ	ısey 🔁	Object Compariso	n			Production Server	• MJN • 🛱 ? બ
mpar	e what? Tasks 🔹 🗹	Compare rules Co	ompare				Records: 27 (filtere
∀=	Task (a) amu ⊽=	Task (b)	Common Si Objects	milarity (%)		Absorbed (%)	
-	AMUpdates01 (2)	AMUpdates02 (2)	1 🗖		33.3%		50.0%
	Object TypeObjectCATAMTKNAM145	Task (a)RulAMUpdates01'ALAMUpdates01'I,J,	L_ACCESS'	Task (b)RAMUpdates02'AAMUpdates02'A	-		
+	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%
-	AMIIndates()? (?)	۵MInterfacec00 (۵)	1	-	11 1%		17 5%
					1 to 27 Next ght (c) 2015		

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**

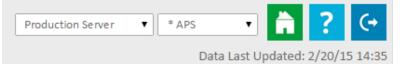
The Security Visualizer provides a graphical representation of your security model. You will be able to drill to security reports at either the User, Role or Security Class (Task) level. Additionally you can assign Roles to Users or Secutity Class to Roles and upload the changes to LS security provide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



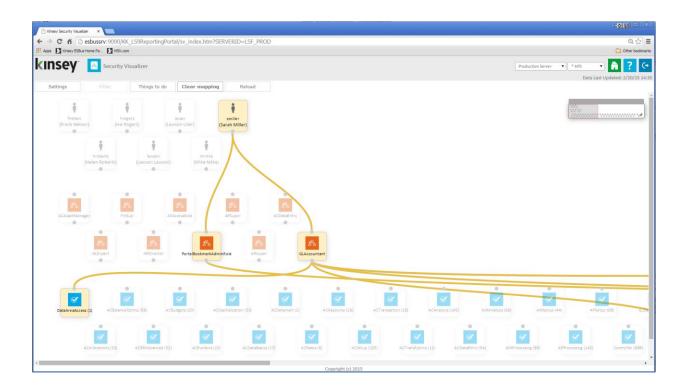
the Security Dashboard from your Windows browser and select the LS Reporting tab and select the Security Visualizer icon.

#### 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.



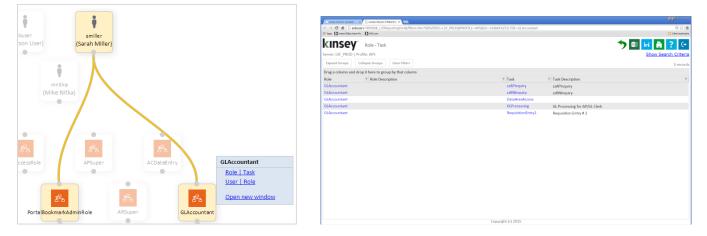
By defaut the application will display a map of the first 100 users in the system and their corresponding Role/Security Class assignments.



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.

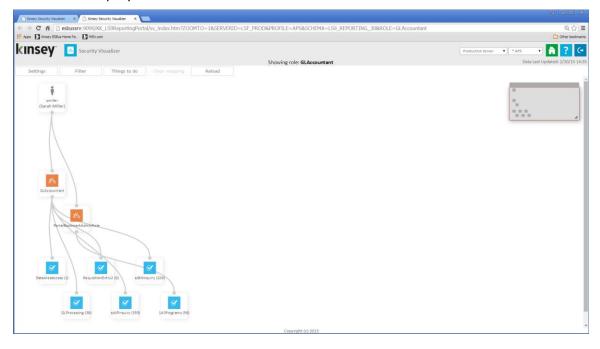
Once you have selected a map you can view specific security settings for any highlighted object.

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.

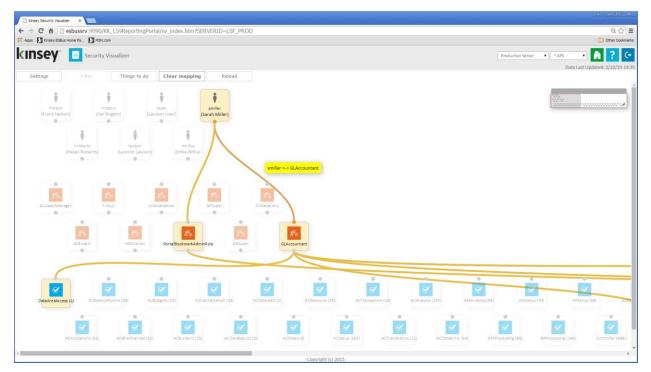
The Has Object option allows you to enter a specific form or table that might be contained in a Security Class. For example if HR11.1 is entered as the Object name all Users, Roles and Security Class linked to HR11.1 will be displayed.

🔏 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.

ок

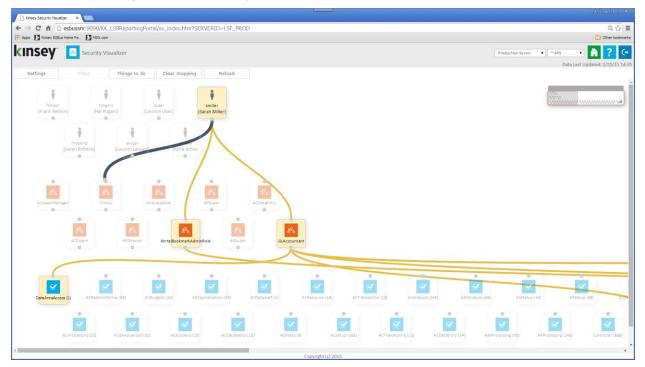
Cancel

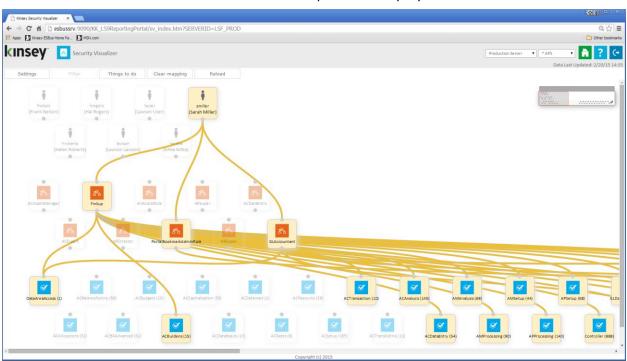
To upload the change click on the <u>Things to do</u> button.

Security Visualize	er			
Filter Th	ings to do Clear mapping	Reload		
	🐁 Utilities	ж	Lawson Security	×
hrogers on) (Hal Rogers)	Upload changes to Lawson		LAWS⊚N <sup>™</sup>	
hroberts	lawson mnitka		User Password	
Provided you have	the credentials to log in th	e 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.

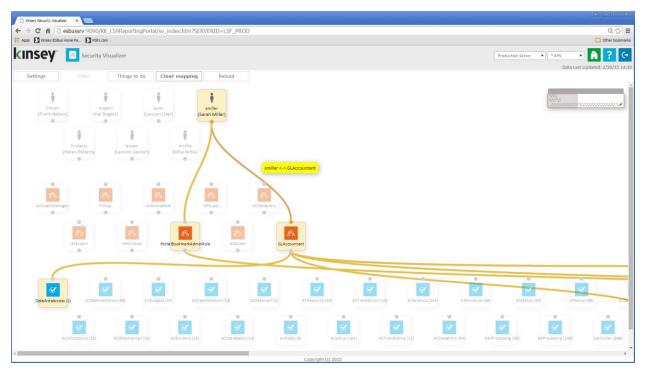
윩	Security Visualiz	er		Lawson Security	×
F	ilter Ti	hings to do Clear mapping	Reload	LAWS@N <sup>*</sup>	
	hrogers	Utilities	*	User   Password	
on)	(Hal Rogers)	opioda changes to caw	301	Add	sk)
hrob	erts	lawson mnitka			

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.

8	Security Visualize	r	Lawson Security *
F	ilter Thi	ngs to do Clear mapping Reload	LAWS@N"
	hrogers	Utilities 🗴	User Password
on)	(Hal Rogers)		Add
hrob	erts	lawson 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.

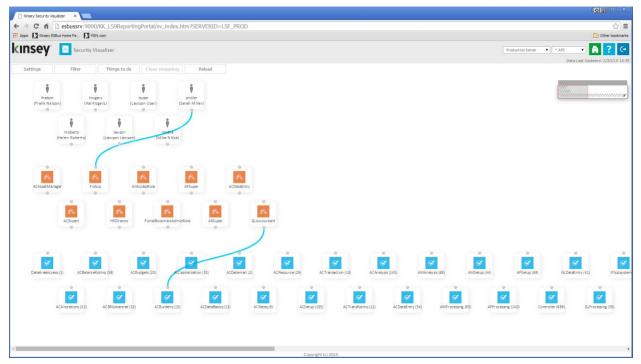
To upload the change click on the <u>Things to do</u> button.

<mark>ه</mark> S	Security Visualizer			With Lawson Security	×
Filt	ter Things	to do Clear mapping	Reload	LAWS	
	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			<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	on Security		×
	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 Securi	nty 9 Reportiny, 🗙 🗅 Kinsey Security Utilities 🛛 🗙 📃	A .	
	59ReportingPortal/util_index.htm?SERVERID=LSF_PROD		© ☆ ≡
Apps 🕒 Kinsey Portal 🚺 MSN.com		<u> </u>	ther bookmarks
kinsey	Security Utilities Production Server • * APS •	?	(→
Clone a task t	to a "read-only" task		
	ACAnalysis - Activity Management Analysist	Task Deta	ails
Task to clone	Refresh	System Codes	0
New task name:	AC Analysis RO	Program Codes	10
New task		Tables	4
description:	AC Analysis Read Only	Forms	91
		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: