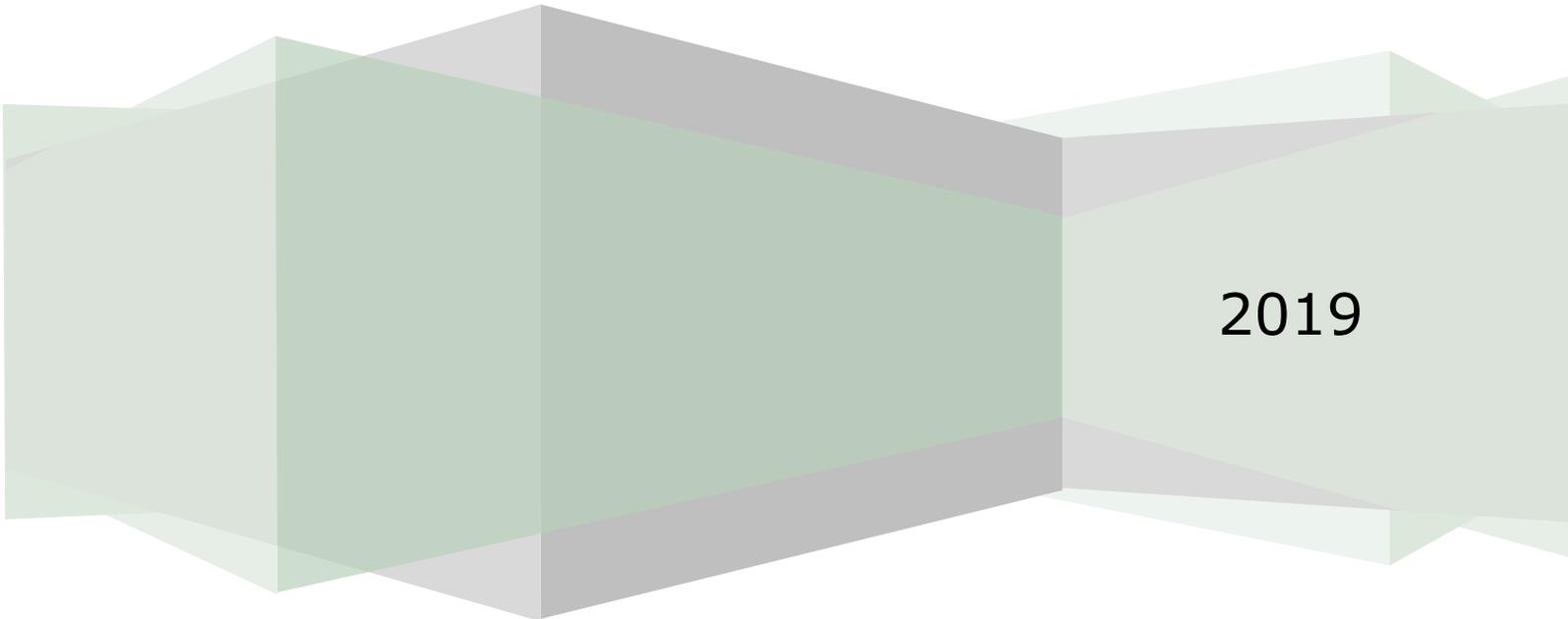




Security Dashboard Users Guide

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

A decorative graphic at the bottom of the page consists of several overlapping, semi-transparent geometric shapes in shades of green and grey, creating a layered, architectural effect.

2019

Contents

Introduction	5
Setting your Default Home Page	6
Configuring your LDAP Reporting Profile	6
Lawson LDAP Server Settings	7
Security Reports	8
Pre-Report Filters	10
Adding or Removing Selected Values	12
Adding or Dropping All Values	13
Filtering the Available Values	14
Changing Pre-Report Filters	15
Showing and Hiding Columns	15
Column Filters	17
Grouping	18
Creating a Group	18
Grouping - Nested	20
Grouping – Expand, Collapse or Remove	20
Grouping – Remove Filters	21
Sorting	21
Adding a Sort Option	21
Removing the Sort Option	21
Saving Reports	22
Saving New Security Reports	22
Changing and Saving an Existing Report	22
Running Saved Report	23
Exporting and Printing	23
Drilling	24
Historical Reporting	26
Historical Comparisons	26
Comparing Profiles	26
Scheduling Security Reports	28
Deleting a Report	29
Security Analyzer	30
Selecting a Server	30
Creating a New Report	31
Filtering by Role	32
Filtering by User	33
Running an Saved Report	33
Editing a Saved Report	34

Deleting a Saved Report	34
Reading the Analyzer Report.....	34
Users Assigned Roles	34
Assigned Forms (TKN).....	35
Assigned Roles and Security Classes.....	35
Assigned Form Conditions	36
Security Auditing	38
Quick Search.....	40
Advanced Search	40
Prompt at Runtime	41
Exporting	42
Creating a MS Excel Document.....	42
Creating a PDF	42
Printing	42
Saving a New Query	42
Saving an Existing Query	43
Scheduling Reports.....	43
Deleting a Report	45
Renaming a Report.....	45
Object Modeling	46
Removing an Object Assignment from a Existing Security Class.....	49
Adding an Object to a New Security Class.....	50
Changing a Forms Function Code Rule.....	51
Linking to Security Reports.....	53
Viewing potential Segregation of Duties violations	54
Role Modeling	55
Changing Role Assignments	56
SOD Validation.....	58
Object Comparison	59
Comparing Role-Security Class Assignments	60
Comparing Role-Security Class Assignments at the Object Level	61
Comparing Security Class Assignments.....	63
Comparing SecurityAssignments at the Object Level	64
Security Visualizer	65
Displaying a User Map.....	66
Settings.....	68
Applying Filters to a User Map	69
Modifying Role Assignments	70

Modifying Security Class Assignments 73
Clear Mapping 76
Security Utilities 77
Trouble Shooting..... 79

Introduction

The Kinsey LS Dashboard provides greater access to information pertaining you user security for both Lawson S3 and Landmark security.

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

The Security Analyzer is specifically built as an audit report for S3 security to easily review access by user. The Microsoft Excel output makes it easy to analyze object level security by user.

The Security Audit report provides details on changes made to your security model including who made the change, when it was made, the object changed and the comparative data of the fields changed.

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



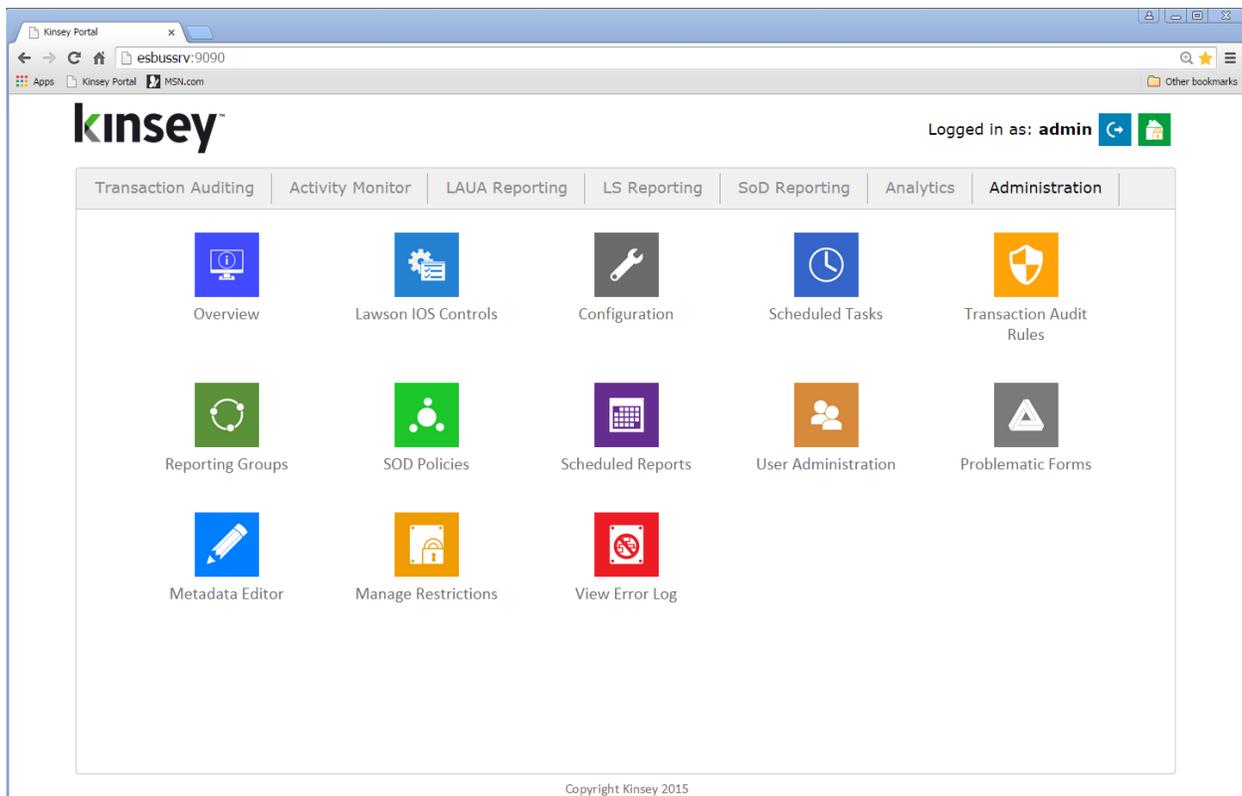
You can set your preferred Home page on the dashboard by selecting the home page icon in the top right corner of your screen. This setting is saved as a browser cookie and will be lost whenever you clear your browser cache.

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: <input type="text" value="ls3server.corpnet.lawson.com"/>	LDAP User: <input type="text" value="CN=root,CN=lwsn,DC=ls3server"/>
LDAP Port: <input type="text" value="389"/>	LDAP Password: <input type="text" value="Lawson1975"/>
LDAP Base Search: <input type="text" value="CN=lwsn,DC=ls3server"/>	LDAP Profile: <input type="text" value="APS"/>
User LDAP Base Search: <input type="text"/>	
LDAP Paging Size: <input type="text" value="1000"/>	RMID Translation Productline: <input type="text"/>
LDAP "back-office" Service: <input type="text"/>	LDAP "Company:Employee" Service: <input type="text" value="LIVE_EMPLOYEE"/>
Collect Employee termination data: <input checked="" type="checkbox"/>	
Employee fields to collect: <input type="text" value="COMPANY;EMPLOYEE;DATE_HIRED;TERM_DA"/>	

Lawson LDAP Server Settings

LDAP Profile: <input type="text" value="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

Collect Employee termination data: <input checked="" type="checkbox"/>
Employee fields to collect: <input type="text" value="COMPANY;EMPLOYEE;DATE_HIRED;TERM_DA"/>

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.

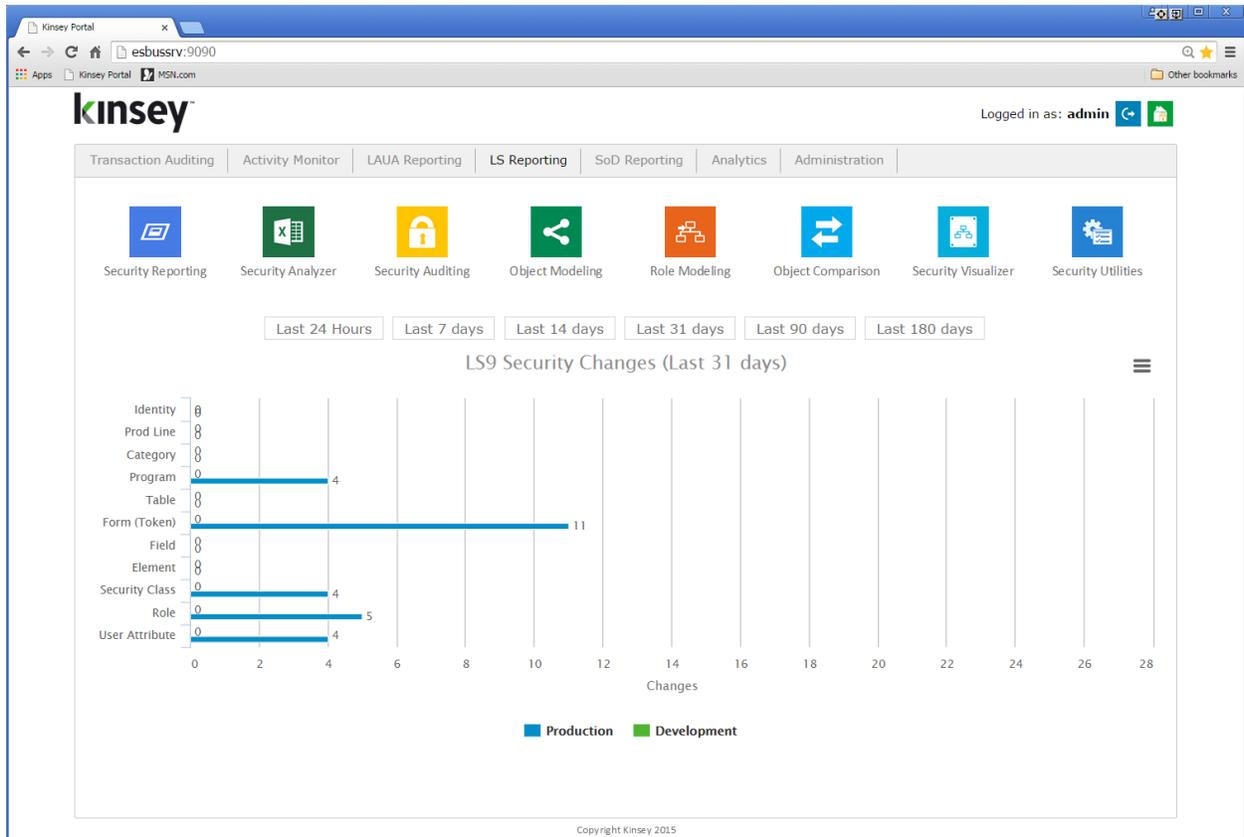
Examples of the fields generally used are: COMPANY, EMPLOYEE, HIRED and TERM_DATE

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

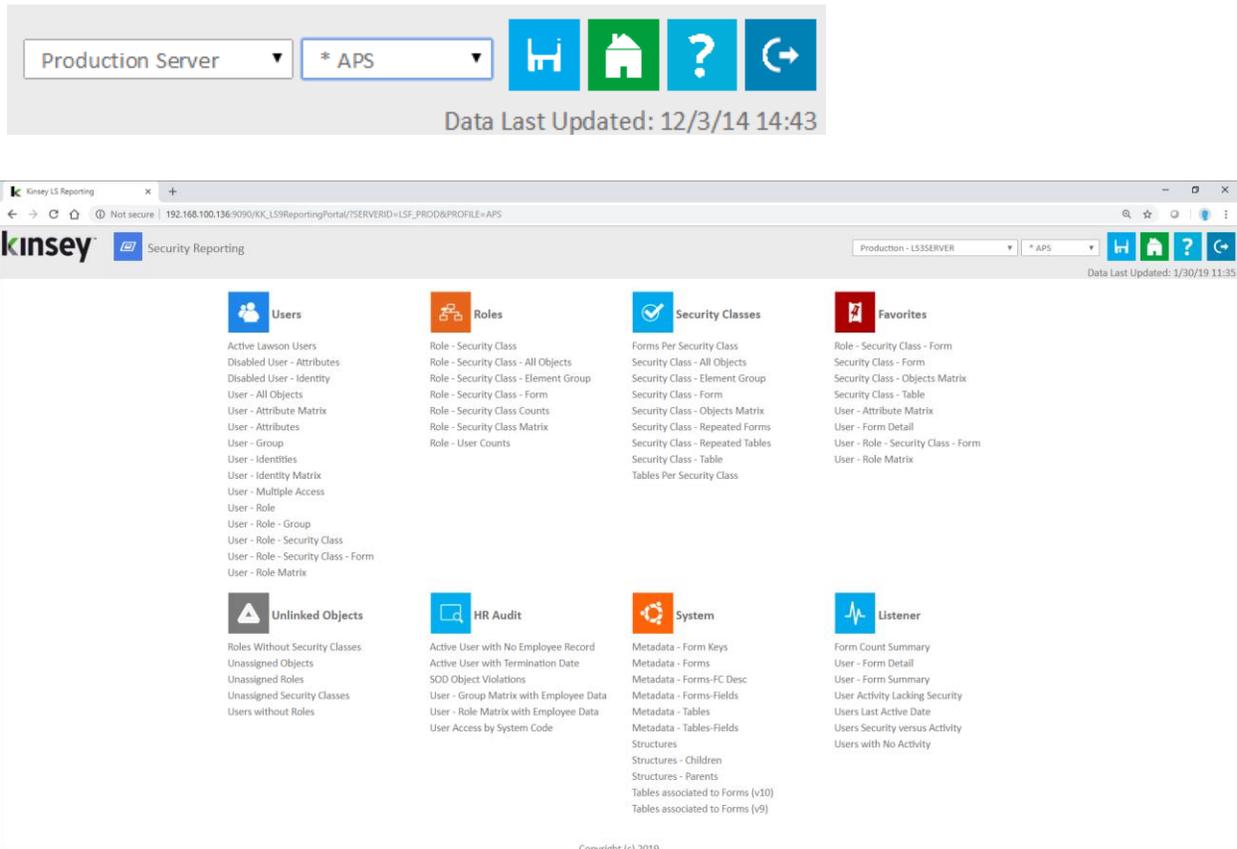
Security Reports

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, Schedule Security Classes for more information.



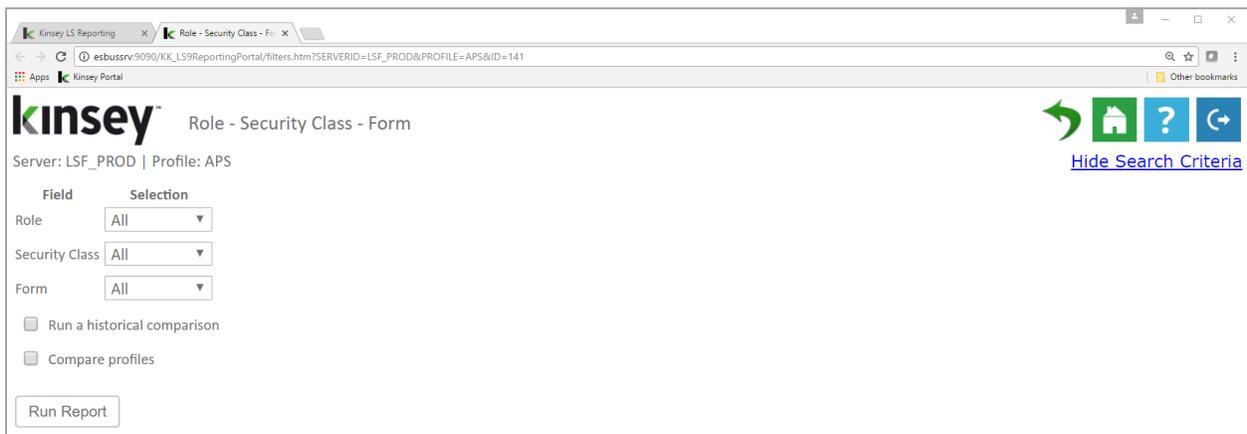
The S3 Security Reporting dashboard comes preconfigured with reports by User, Role, Security Class and System information about your model. If you are licenses for the Activity Monitor (Listener) application a separate group of reports will provide you will information on how Lawson is being used.

Report Features

Pre-Report Filters

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

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



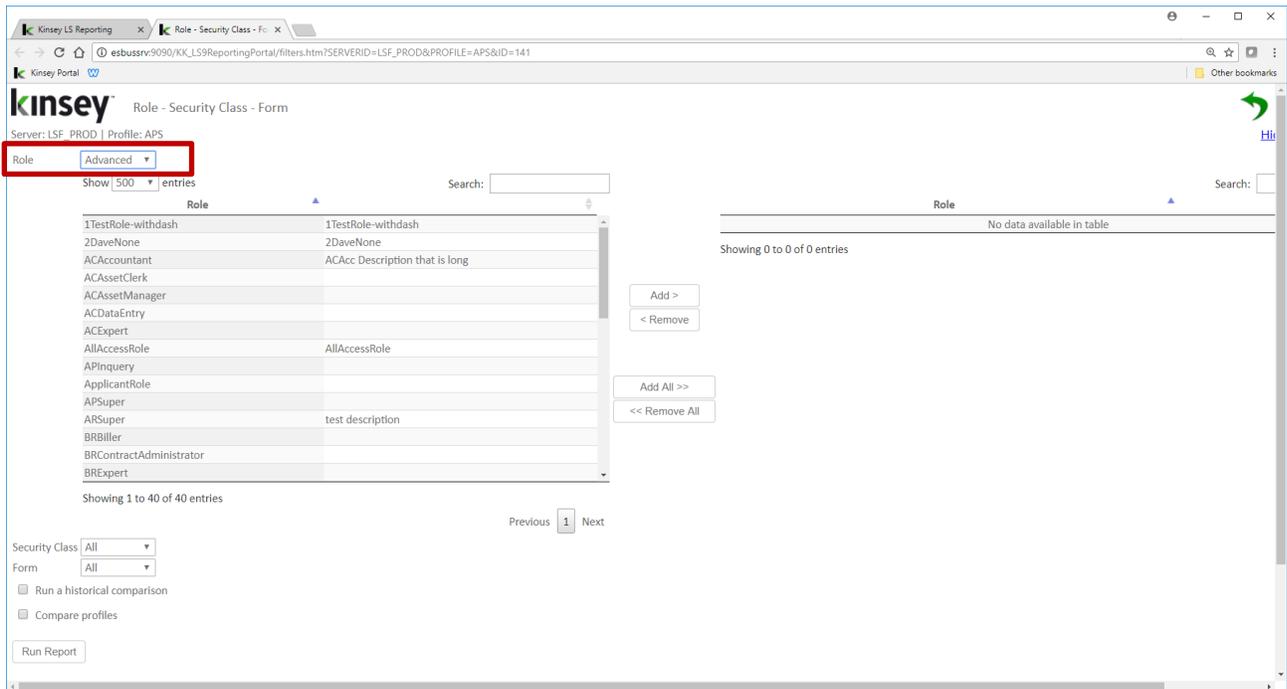
For example, on the Role – Security Class – Form report you will have the option of filtering by Role, Security Class or Form. If you need to filter by any other field you can do that once the grid is populated. All filters assume “AND” logic, meaning all values must satisfy the criteria for data to 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 Between	Date returned must fit within the range selected.
Regular-Ex	Similar to OR logic. Entered as value value value etc. This is useful when trying to view records with specific dates.

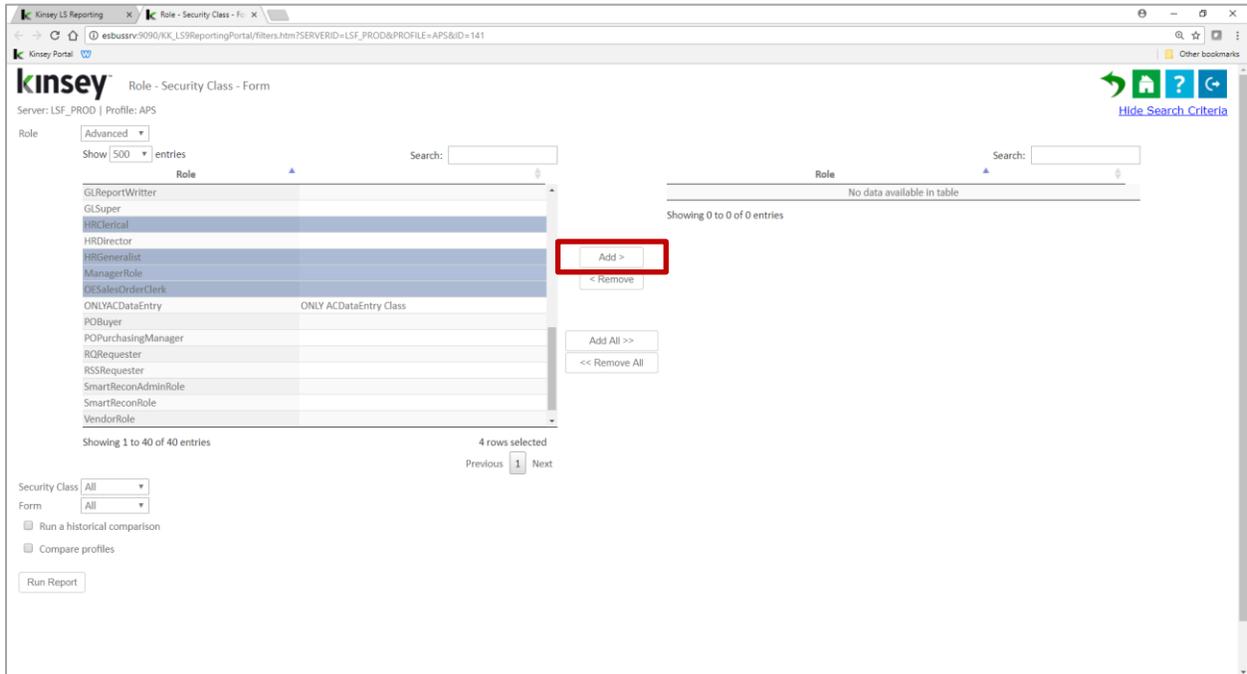
The second method allows you to select from a list of possible values. This option can take a little time to populate depending on the size of the model. The values shown are based on the information available in your security model.



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 available Roles are displayed. At this point you have a few ways of selecting the Roles you would like included on the report.

Adding or Removing Selected Values

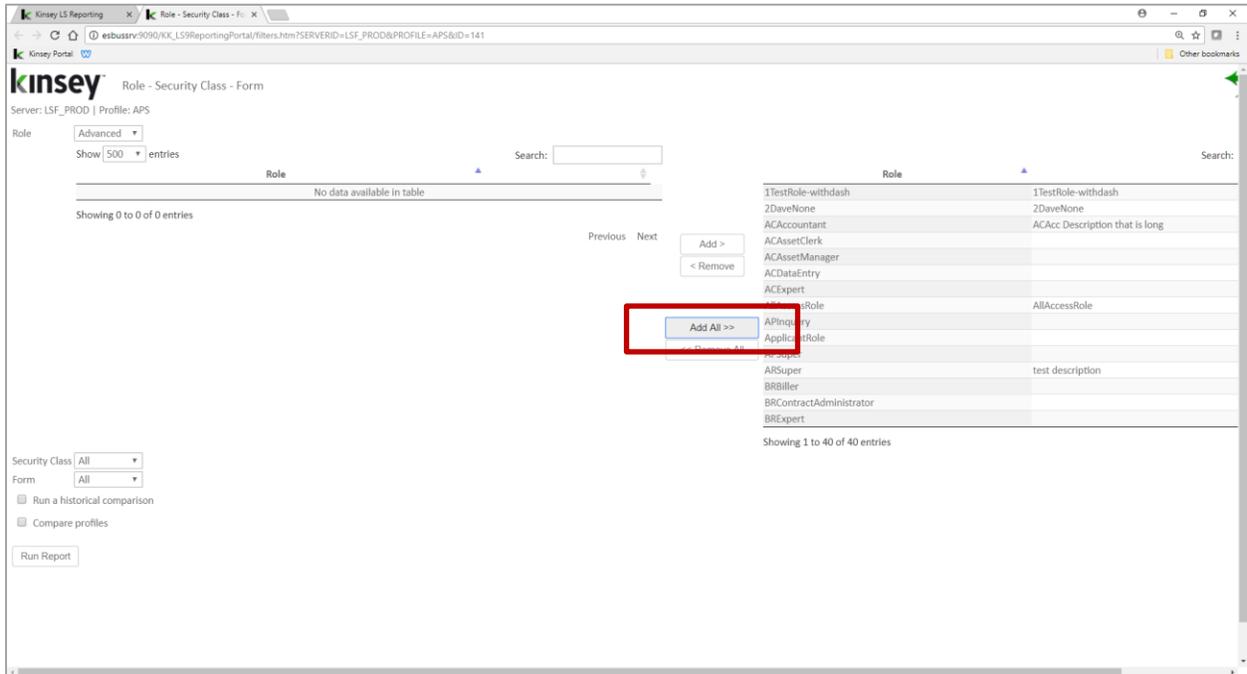
By holding down the CTRL key you can select individual values or by holding down the Shift key you can select a range of values you want included on the report. Clicking the **Add >** button will move the selections to the selected column. To remove a values from the list select the items in the 'Selected' column and click on **< Remove**.



Adding or Dropping All Values

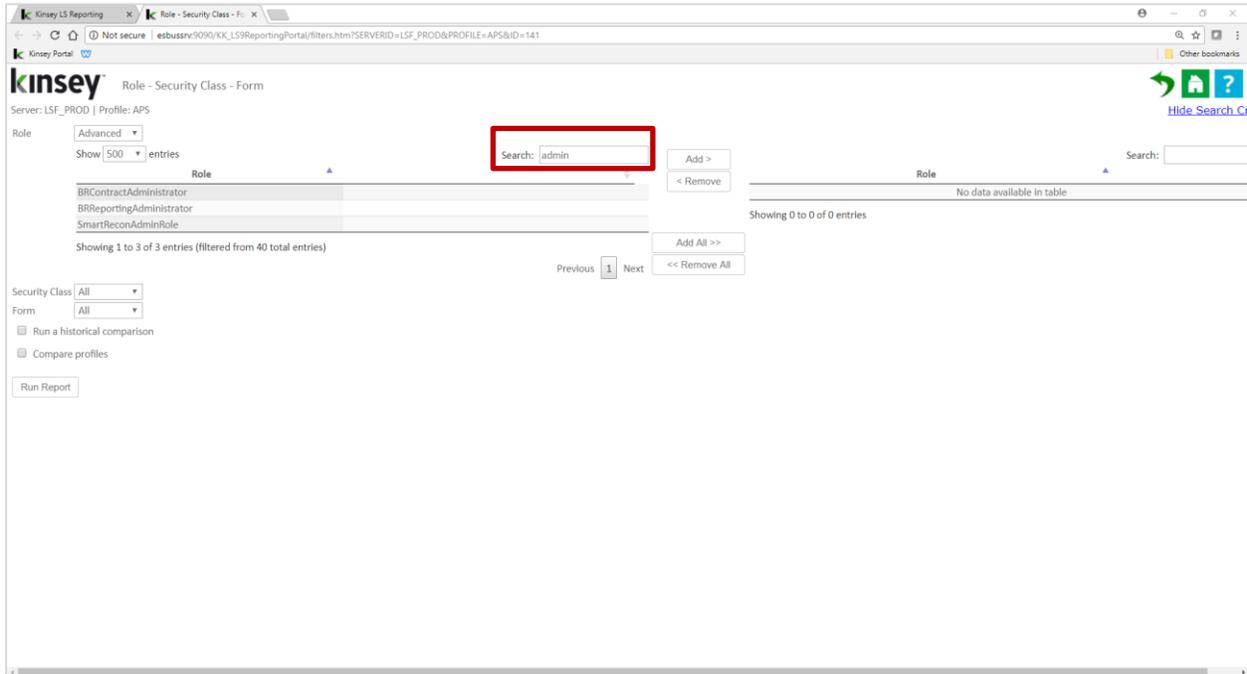
To add all values simply click on the **Add All >>** button. To remove all select the **<< Remove All** button.

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



Filtering the Available Values

The “Search” box will allow you to filter the list of entries displayed. The application used “contains” logic to filter the data.

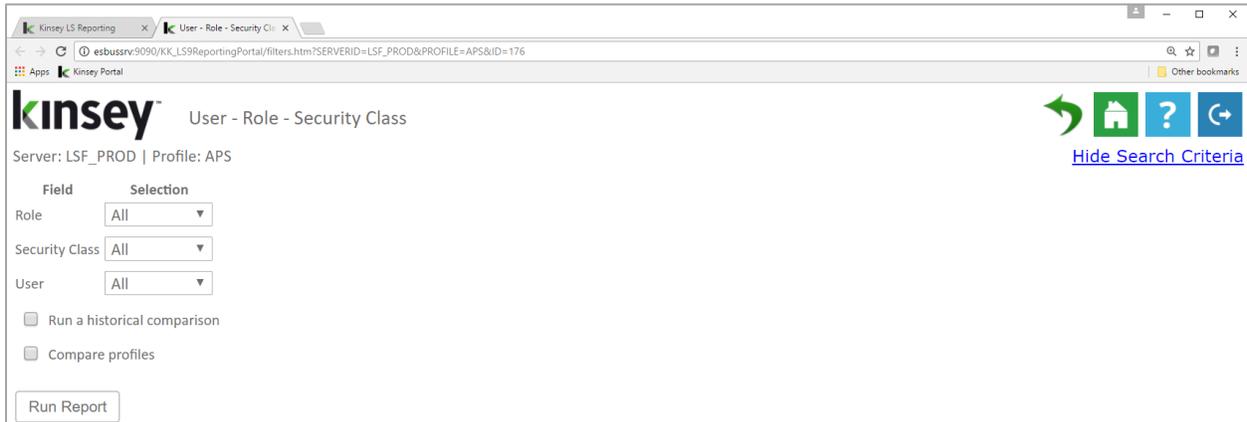


In this example, to display all of the roles related to an Administrator I entered ‘admin’ in the search box. At this point I can click on the Add All button to move them to the selected list. You can remove items from the selected list by entering a condition and selecting the << **Remove All** button.

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 containing “admin” and then also Add all values containing “super”.

Changing Pre-Report Filters

To change your selection criteria without exiting the report simply select the Show/Hide Search Criteria link in the upper right corner of your screen.



Showing and Hiding Columns

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

Note: not all fields show on all reports

Overview

- Lawson IOS Controls
- Configuration
- Scheduled Tasks
- Transaction Audit Rules
- Reporting Groups
- SOD Policies
- Scheduled Reports
- User Administration
- Problematic Forms
- Metadata Editor
- Manage Restrictions
- View Error Log

LS9 Security Configuration (Production Server)

LDAP Server:

LDAP Port:

LDAP Base Search:

User LDAP Base Search:

LDAP Paging Size:

LDAP "back-office" Service:

Collect Employee termination data:

Employee fields to collect:

Hidden	Friendly Name	Database Field
<input type="checkbox"/>	Attribute	ATTRIBUTE
<input type="checkbox"/>	Attribute Value	ATTRIBUTE_VALUE
<input type="checkbox"/>	Audit	AUDITED
<input type="checkbox"/>	Available FC	AVAILABLEFC
<input type="checkbox"/>	Check LS	CHECK_LS
<input type="checkbox"/>	Company	COMPANY
<input type="checkbox"/>	Count	ListenerCount
<input type="checkbox"/>	Date	DATE
<input type="checkbox"/>	Date	ACCESSED_AT_DATE
<input type="checkbox"/>	Date/Time	ACCESSED_AT
<input type="checkbox"/>	Employee	EMPRNUM
<input type="checkbox"/>	Field Description	LABEL
<input type="checkbox"/>	Form	TOKEN
<input type="checkbox"/>	Form Description	TITLE
<input type="checkbox"/>	Full Name	FULLNAME
<input type="checkbox"/>	Function	FC
<input type="checkbox"/>	Hidden	HIDDEN

Column Filters

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

Role	Role Description	Security Class	Security Class Description	Form	Form Description	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...	AC00.1	Status	+,-,A,C,I	'C,I,+,-'
ACAccountant	ACAcc Description th...	ACAnalysis	Activity Managemen...	AC00.3	Resource	A,C,D,I,N,P	'I'
ACAccountant	ACAcc Description th...	ACAnalysis	Activity Managemen...	AC00.2	AC Person Assignme...	+,-,A,C,I,N,P	'I'
ACAccountant	ACAcc Description th...	ACAnalysis	Activity Managemen...	AC00.3	HR Employee Assign...	+,-,A,C,I,N,P	'I'
ACAccountant	ACAcc Description th...	ACAnalysis	Activity Managemen...	AC00.4	Vendor Assignment	+,-,A,C,I,N,P	'I'
ACAccountant	ACAcc Description th...	ACAnalysis	Activity Managemen...	AC00.5	Asset Assignment	+,-,A,C,I,N,P	'I'
ACAccountant	ACAcc Description th...	ACAnalysis	Activity Managemen...	AC00.6	Equipment Assignm...	+,-,A,C,I,N,P	'I'
ACAccountant	ACAcc Description th...	ACAnalysis	Activity Managemen...	AC00.7	Role Assignment	+,-,A,C,D,I,N...	'I'
ACAccountant	ACAcc Description th...	ACAnalysis	Activity Managemen...	AC00.8	Roles	+,-,A,C,I	'I'
ACAccountant	ACAcc Description th...	ACAnalysis	Activity Managemen...	AC00.9	Resource Account	C,I	'I'
ACAccountant	ACAcc Description th...	ACAnalysis	Activity Managemen...	AC00.1	GL Code	+,-,A,C,I	'I'
ACAccountant	ACAcc Description th...	ACAnalysis	Activity Managemen...	AC00.5	Account Categories	NO FC	'I'
ACAccountant	ACAcc Description th...	ACAnalysis	Activity Managemen...	AC00.6	Override Account Ca...	+,-,C,I,N,P	'ALL_ACCESS'
ACAccountant	ACAcc Description th...	ACAnalysis	Activity Managemen...	AC00.2	Override Mass Add/...	A,C,I	'I'

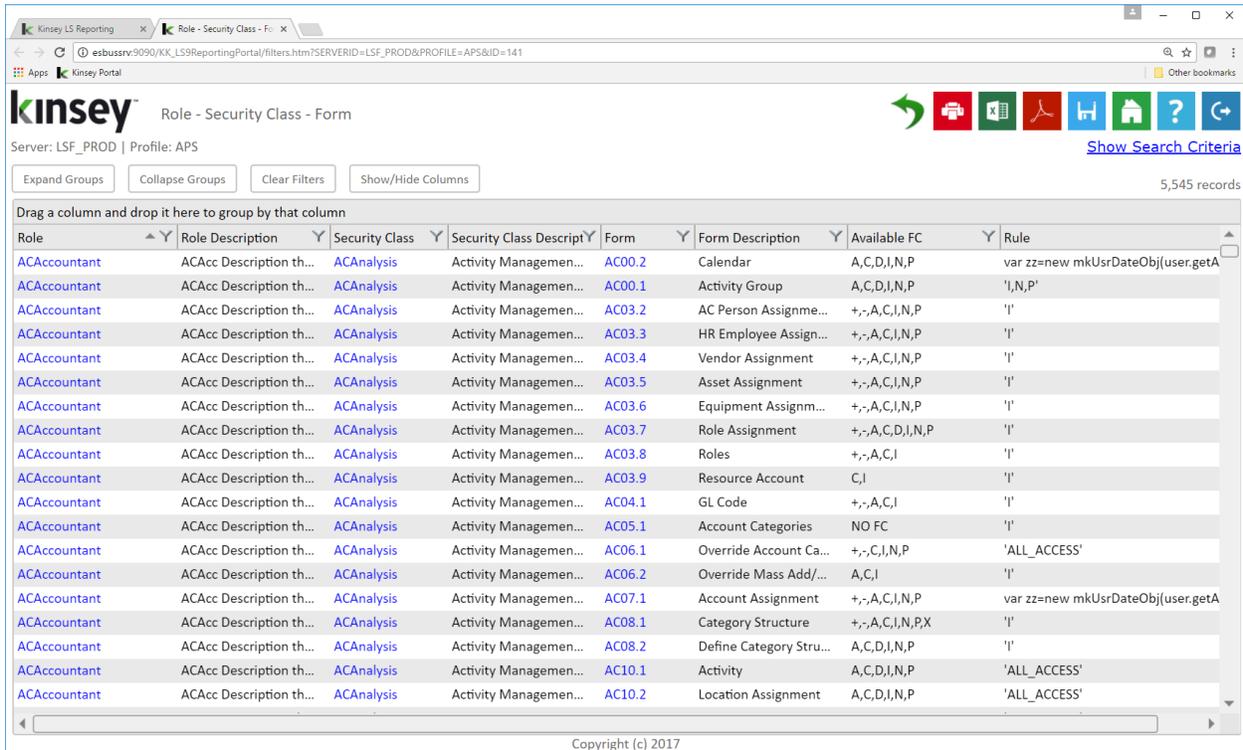
- Sort Ascending
- Sort Descending
- Remove Sort
- Group By this column
- Remove from groups
- Show rows where:
-
-
- And
-
-

Each column 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 expression and enter the value. The expressions 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 logic select the down arrow next the word ‘And’ and change the option to ‘OR’.

Grouping

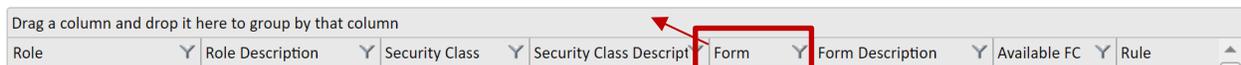
Creating a Group

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.

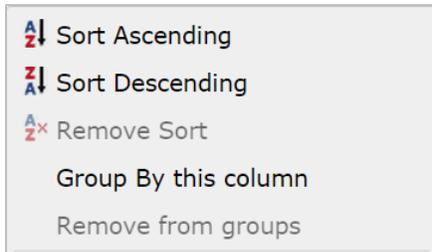


Let's take a look at the following query for Role – Security Class - Form. By default this query is going to be displayed in detail by Role, Class and Form. But let's say we want to rearrange the list and group it by Form to see all of the Security Classes and Roles assigned to each Form.

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.



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.

Form	Role	Role Description	Security Class	Security Class Description	Form	Form Description	Available FC	Rule
▶	Form: CU01.1	(12)						
▶	Form: AC00.1	(12)						
▶	Form: AC00.2	(12)						
▶	Form: AC02.1	(8)						
▶	Form: AC03.1	(8)						
▶	Form: AC03.2	(8)						
▶	Form: AC03.3	(8)						
▶	Form: AC03.4	(8)						
▶	Form: AC03.5	(8)						
▶	Form: AC03.6	(8)						
▶	Form: AC03.7	(8)						
▶	Form: AC03.8	(8)						
▶	Form: AC03.9	(8)						
▶	Form: AC04.1	(7)						
▶	Form: AC05.1	(7)						

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.

Form	Role	Role Description	Security Class	Security Class Description	Form	Form Description	Available FC	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	'I'
	ACAccountant	ACAcc Description th...	ACDataEntry	Activity Managemen...	AC03.1	Resource	A,C,D,I,N,P	'I'
	ACAssetClerk		ACAnalysis	Activity Managemen...	AC03.1	Resource	A,C,D,I,N,P	'I'
	ACDataEntry		ACAnalysis	Activity Managemen...	AC03.1	Resource	A,C,D,I,N,P	'I'
	ACExpert		ACResource	AC Resources, Roles,...	AC03.1	Resource	A,C,D,I,N,P	'ALL_ACC'
	FinSup		ACAnalysis	Activity Managemen...	AC03.1	Resource	A,C,D,I,N,P	'I'
	FinSup		ACDataEntry	Activity Managemen...	AC03.1	Resource	A,C,D,I,N,P	'I'
	ONLYACDataEntry	ONLY ACDataEntry C...	ACDataEntry	Activity Managemen...	AC03.1	Resource	A,C,D,I,N,P	'I'
▶	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.

Form	Role	Role Description	Security Class	Security Class Description	Form	Form Description	Available FC	Rule
Form: CU01.1 (4)								
Form: AC00.1 (3)								
Form: 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	var
FinSup			ACAnalysis	Activity Managemen...	AC00.2	Calendar	A,C,D,I,N,P	var
Security Class: ACDataEntry (3)								
Security Class: ACSetup (5)								
Form: AC02.1 (3)								
Form: 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 Security Class.

Grouping – Expand, Collapse or Remove

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



Simply select the Expand or Collapse buttons to display or hide the grouping details. To remove a group entirely 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

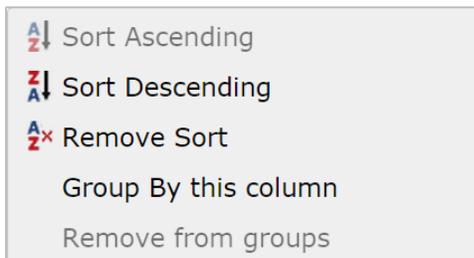
Adding a Sort Option

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 drop it here to group by that column

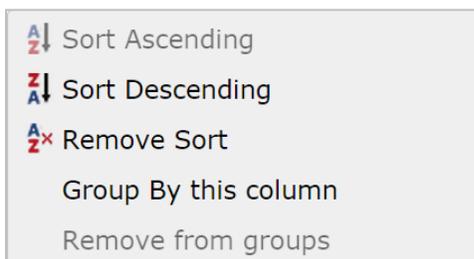
Role	Security Class	Security Class Description	Form	Form Description	Available FC	Rule
ACAssetClerk	ACAnalysis	Activity Managemen...	AC00.1	Activity Group	A,C,D,I,N,P	'I,N,P'
ACAccountant	ACAnalysis	Activity Managemen...	AC00.1	Activity Group	A,C,D,I,N,P	'I,N,P'
FinSup	ACAnalysis	Activity Managemen...	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	'I'
ONLYACDataEntry	ACDataEntry	Activity Managemen...	AC00.1	Activity Group	A,C,D,I,N,P	'I'
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.



Removing the Sort Option

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

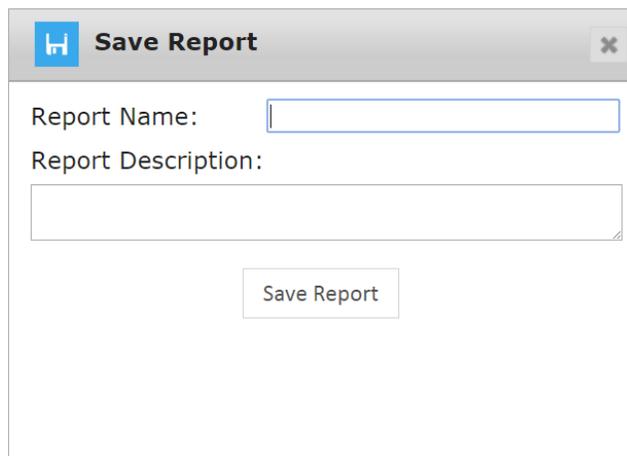


Saving Reports

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 Report

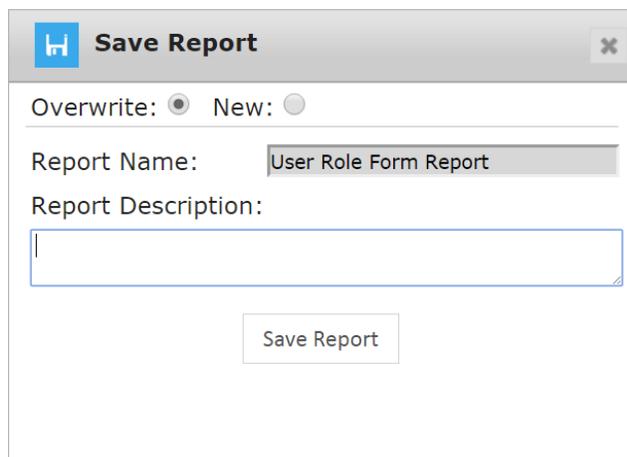
Report Name:

Report Description:

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 Report

Overwrite: New:

Report Name:

Report Description:

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 or 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 (up to 3 levels), 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.

1	A	B	C	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						
	7825						

Drilling

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

To execute a drill click on the linked object you need to review. In the example below I clicked on the **HRGeneralist** Role and was provided the option of viewing the Security Classed assigned to HRGeneralist or the Users that have been assigned the HRGeneralist Role.

Drag a column and drop it here to group by that column							
Role	Security Class	Security Class Description	Form	Form Description	Available FC	Rule	
HR Clerical	HRSetupInq	Inquiry only access t...	HR00.1	Company	A,C,D,I,N,P	'I,N,P'	
HR Director	HRSetup	All Access to HR Setu...	HR00.1	Company	A,C,D,I,N,P	'ALL_ACCESS'	
HR Clerical	HRSetup	All Access to HR Setu...	HR00.1	Company	A,C,D,I,N,P	'ALL_ACCESS'	
HRGeneralist	HRSetup	All Access to HR Setu...	HR00.1	Company	A,C,D,I,N,P	'ALL_ACCESS'	
HR Clerical	HRSetupInq	Inquiry only access t...	HR00.2	Canada Payroll Acco...	+,-,A,C,I	'I,N,P,+,-'	
HR Clerical	HRSetup	All Access to HR Setu...	HR00.2	Canada Payroll Acco...	+,-,A,C,I	'ALL_ACCESS'	
HR Director	HRSetup	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 Security Classes assigned to this Role.

Drag a column and drop it here to group by that column			
Role	Role Description	Security Class	Security Class Description
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 Class.

Drag a column and drop it here to group by that column

Security Class	Security Class Description	Form	Form Description	Available FC	Rule
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 column

Role	Security Class	Security Class Description
ACAssetClerk	ACSetup	Activity Management Setup
ACAssetClerk	ACTransaction	Activity Management Transaction Entry, Posting
ACAssetClerk	AMPProcessing	Asset Management Processing
ACAssetClerk	AMSetup	Asset Management Setup
ACAssetClerk	PRFiles	PR Files
ACAssetManager	ACSetup	Activity Management Setup
ACAssetManager	ACAssetManager	AC Asset Manager
ACBRJobScheduler	ACBRJobScheduler	AC and Br Job Scheduler Jobs
ACBRJobScheduler	DataAreaAccess	Data Area Access
ACDataEntry	ACAnalysis	Activity Management Analyst
ACDataEntry	ACBalanceRptInq	Activity Management Balance Reports, Inquiries
ACDataEntry	DataAreaAccess	Data Area Access
ACExpert	ACAllocations	Activity Management Allocation Processing
ACExpert	ACBalanceRptInq	Activity Management Balance Reports, Inquiries

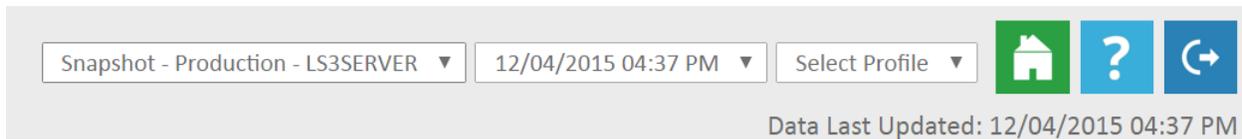
The User | Role option will display a list of the User's assigned to this Role.

Drag a column and drop it here to group by that column

User	Full Name	Role	Role Description
bthomas	Thomas, Bill	ACAssetManager	
schristian	Christian, Sammy	ACAssetManager	

Historical Reporting

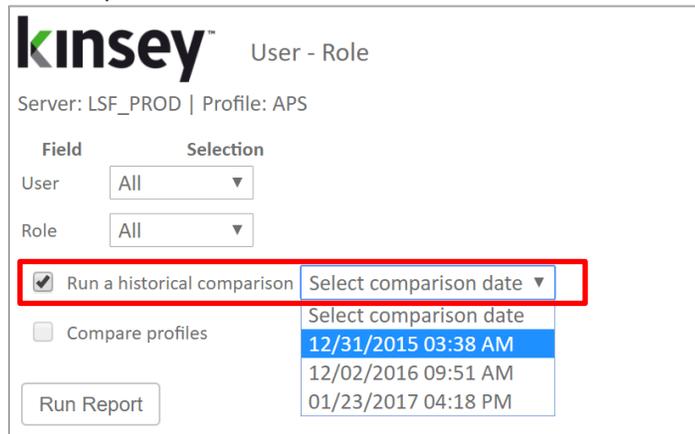
Historical Reports support all of the functionality found in the standard reports. You can either chose to run historical reports by selecting the appropriate Snapshot and Profile in the top right corner of the screen or you can compare your current security settings to a prior snapshot. To run historical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



Note: The majority of the Security Reports will be available, however not all data is timestamped so some reports may not be available.

Historical Comparisons

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 select a report you will have the option to select a Snapshot for the comparison.



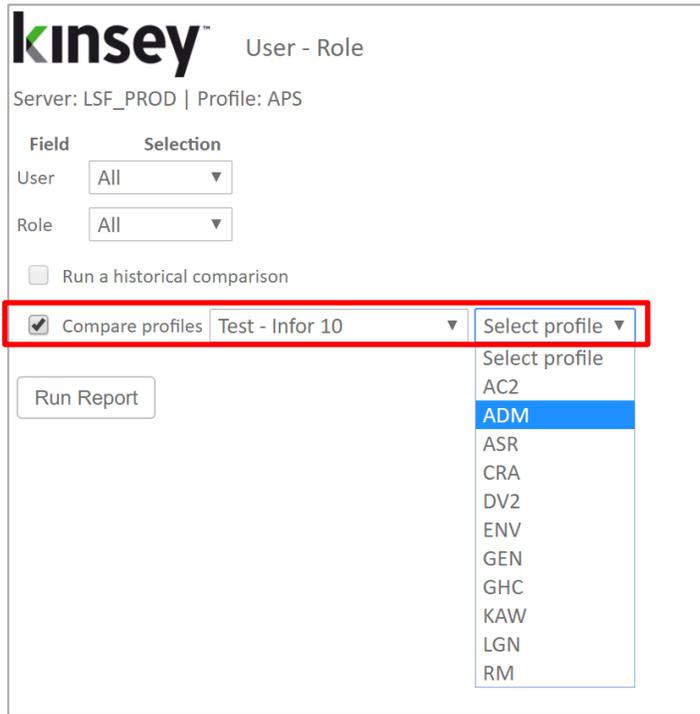
Note: You can only compare historical snapshot to your existing security settings, you cannot compare snapshots.

For more information on how to create Historical snapshots refer to the Kinsey Administrator Guide, Scheduled Security Classes.

Comparing Profiles

The profile comparison option allows you to compare 2 profiles on the same server or across 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 select 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.



The screenshot shows the Kinsey User - Role interface. At the top left is the Kinsey logo. To its right is the text 'User - Role'. Below this, it says 'Server: LSF_PROD | Profile: APS'. There are two dropdown menus: 'User' with 'All' selected and 'Role' with 'All' selected. Below these is a checkbox labeled 'Run a historical comparison' which is unchecked. A red box highlights a checked checkbox labeled 'Compare profiles', followed by a dropdown menu showing 'Test - Infor 10' and another dropdown menu labeled 'Select profile'. This 'Select profile' dropdown is open, showing a list of profile names: 'Select profile', 'AC2', 'ADM' (highlighted in blue), 'ASR', 'CRA', 'DV2', 'ENV', 'GEN', 'GHC', 'KAW', 'LGN', and 'RM'. Below the 'Compare profiles' section is a 'Run Report' button.

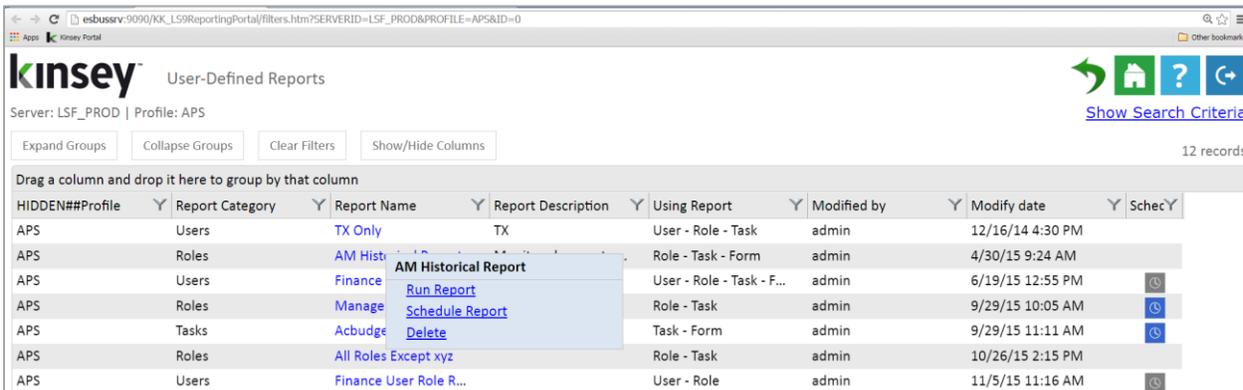
For more information on how to create Historical snapshots refer to the Kinsey Administrator Guide, Scheduled Security Classes.

Scheduling Security Reports

Scheduling a report will allow you to automatically email any report you would like to receive on a regular basis. Start by selecting the save icon on the Security Reporting.



Once the report displays on the saved reports page you can click on the report name and select **Schedule Report**.



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.

NOTE: The schedule must be enabled for the schedule to run. To enable a scheduled report refer to the Schedule Reports section of the Administrators Guide.

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. For a new schedule enter a schedule name, frequency and run time.

Schedule Report
✕

Finance Group Security Report

Select schedule to use: Select existing Create new schedule

Schedule name:

Every at :

Select users to email: Select existing Create new group

Email group name:

Email format: ▼

Send reports with no changes:

Cancel
Save

You can also create or use existing report groups. A report group contains a list of users you want to receive the report. Each user address should be separated by either a comma or a semicolon.

Note: do not insert a return between names in the list.

The screenshot shows a 'Schedule Report' dialog box with the following fields and options:

- Select schedule to use:** Radio buttons for 'Select existing' and 'Create new schedule' (selected).
- Schedule name:** Text input field containing 'Daily'.
- Frequency:** 'Every' dropdown set to 'day', 'at' dropdown set to '20', and '00'.
- Select users to email:** Radio buttons for 'Select existing' and 'Create new group' (selected).
- Email group name:** Text input field containing 'Finance'.
- Email addresses:** Text area containing 'd.kinsey@kinsey.com;m.nitka@kinsey.com'.
- Email format:** Dropdown menu set to 'Excel 2007 (and above) (*.xlsx)'.
- Send reports with no changes:** Checked checkbox.
- Buttons:** 'Cancel' and 'Save' buttons at the bottom.

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 recipient that the report was run.

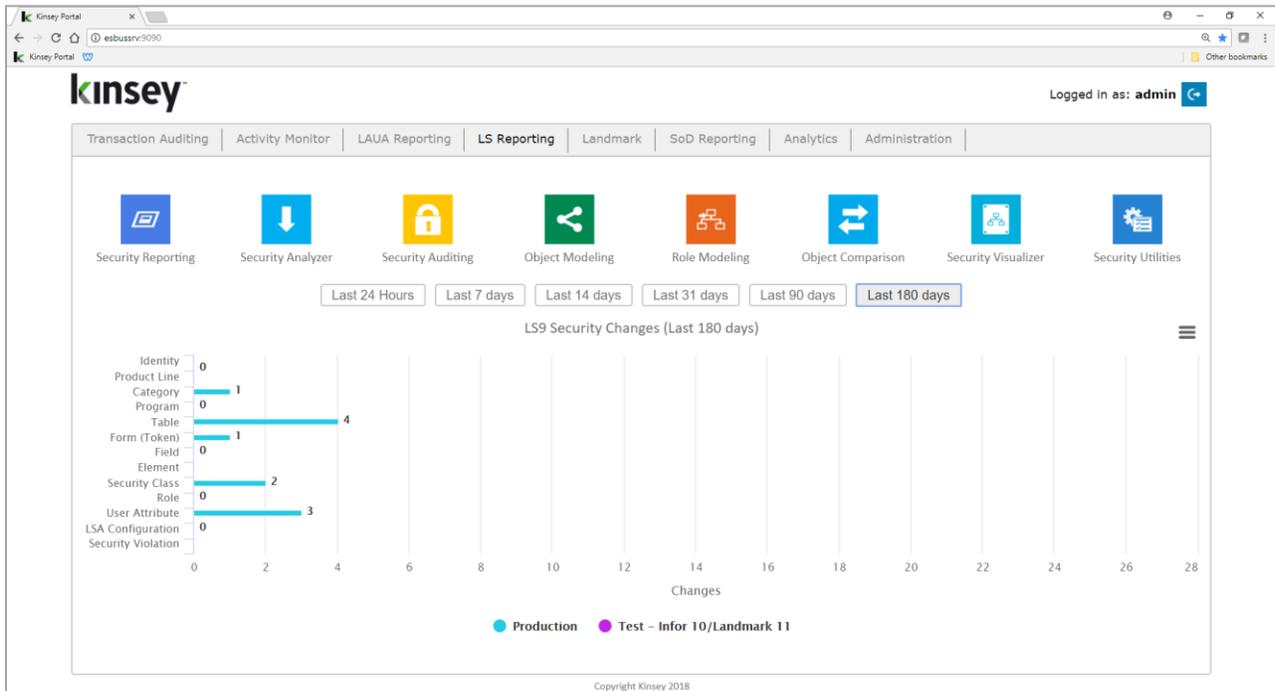
Deleting a Report

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

Security Analyzer

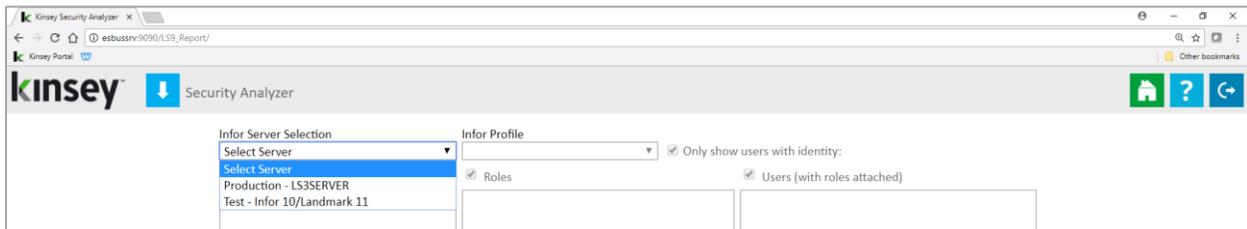
The Security Analyzer is designed specifically for anyone that needs to audit security functionality in the S3 (LDAP) model. Although these reports can be used by the security administrator, they can only be run at the user level. Reports on how Roles and Security Classes are defined are part of the 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 and profile containing your security 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 and Users to choose from.



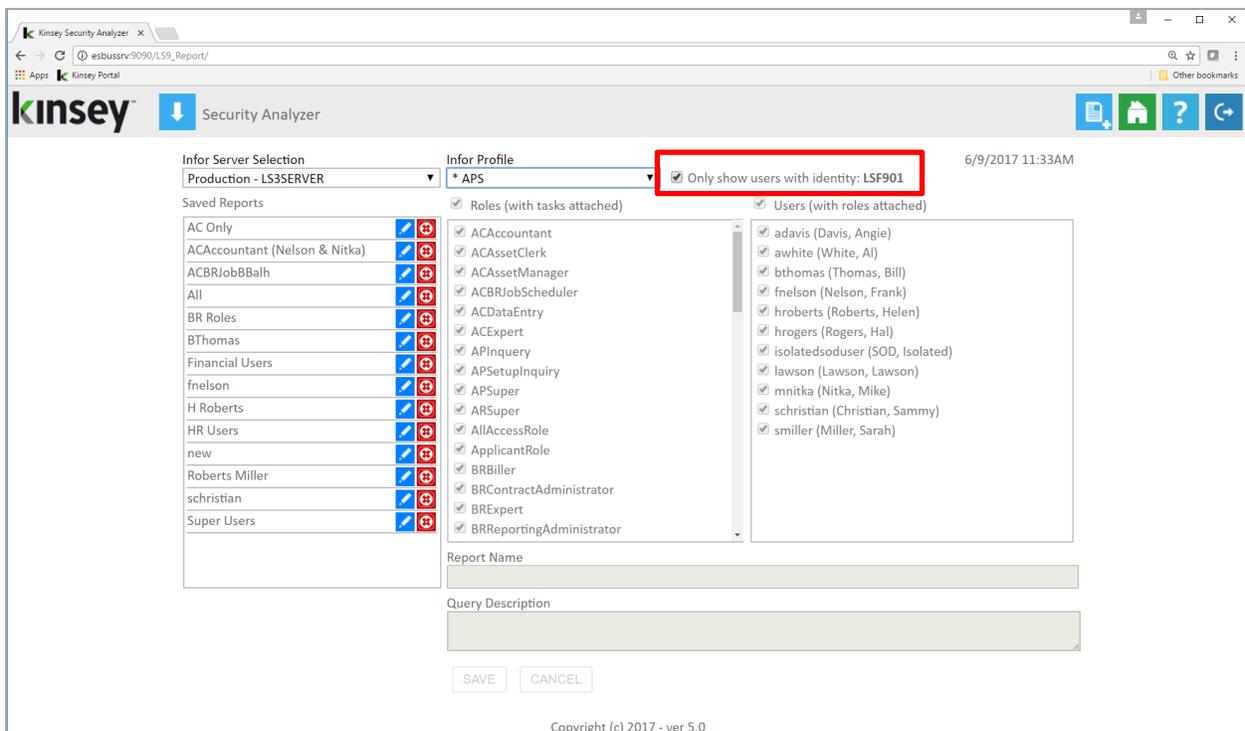
Creating a New Report

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 or Users when 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 in Lawson Security the user list will change automatically the next time you run the report. The alternative is to select the User's manually to create a static list of users.

Note: Self-Service only users can be added to this report by unchecking the "Only show users with identity:" checkbox.



Filtering by Role

Start by unchecking the Roles checkbox shown above the Role list. This will unselect each Role so you can manually select the Roles associated with the Users you want to see on the report. In the example below when Roles BRBiller and BatchRole are selected a list of users assigned with either one of these roles is displayed on the right. These will be the users shown on the report.

Infor Profile 3/6/2018 1:21PM

* APS Only show users with identity: LSF901

<input type="checkbox"/> Roles	<input checked="" type="checkbox"/> Users (with roles attached)
<input type="checkbox"/> ApplicantRole	<input checked="" type="checkbox"/> adavis (Davis, Angie)
<input type="checkbox"/> AshantiTestRole	<input checked="" type="checkbox"/> awhite (White, Al)
<input checked="" type="checkbox"/> BRBiller	<input checked="" type="checkbox"/> bthomas (Thomas, Bill)
<input type="checkbox"/> BRContractAdministrator	<input checked="" type="checkbox"/> hroberts (Roberts, Helen)
<input type="checkbox"/> BRExpert	<input checked="" type="checkbox"/> hrogers (Rogers, Hal)
<input type="checkbox"/> BRReportingAdministrator	<input checked="" type="checkbox"/> lawson (Lawson, Lawson)
<input type="checkbox"/> BRRevenueAnalyst	<input checked="" type="checkbox"/> mnitka (Nitka, Mike)
<input checked="" type="checkbox"/> BatchRole	<input checked="" type="checkbox"/> schristian (Christian, Sammy)
<input type="checkbox"/> BestPracticeRole	<input checked="" type="checkbox"/> smiller (Miller, Sarah)
<input type="checkbox"/> CU01InheritedHR11	
<input type="checkbox"/> CustomerRole	
<input type="checkbox"/> DESKTOP	
<input type="checkbox"/> DESKTOPFiles	
<input type="checkbox"/> DEVINQ	
<input type="checkbox"/> DEVINQFiles	
<input type="checkbox"/> DaveRole	

Note: The report will include all security information for the users listed. The report will not be limited to the Roles selected. The purpose of selecting Roles is to identify the associated users.

Filtering by User

Start by unchecking the User checkbox shown above the User list. This will unselect each User so you can manually select the User's you want to see on the report.

Infor Profile
3/6/2018 1:21PM

* APS

Only show users with identity: LSF901

Roles

Users (with roles attached)

ACAccountant
 APInquiry
 APSetupInquiry
 AllAccessRole
 BatchRole
 ESSPortalRole
 EntryClerk
 FinSup
 FinancialRole
 ONLYACDataEntry
 PortalBookmarkAdminRole
 ProcessFlowRole
 rSubAdminRole

adavis (Davis, Angie)
 awhite (White, Al)
 bthomas (Thomas, Bill)
 fnelson (Nelson, Frank)
 hroberts (Roberts, Helen)
 hrogers (Rogers, Hal)
 isolatedsoduser (SOD, Isolated)
 lawson (Lawson, Lawson)
 mnitka (Nitka, Mike)
 schristian (Christian, Sammy)
 smiller (Miller, Sarah)

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. The report can be generated in Microsoft Excel or as a PDF document and may appear at the bottom of your browser page depending on the browser being used.

↓
Download results as:
✕

Microsoft Excel

Run Report

Abobe PDF

Run Report

Select your preferred format.

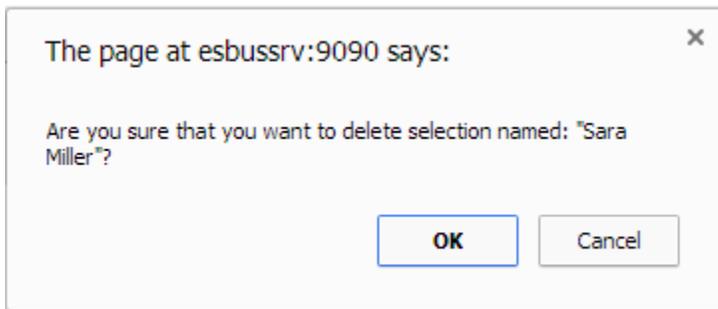
Once the generation process is complete you will see an option to download the Excel document in the lower left corner of the selection screen under the Report Options section.

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

Summary of Lawson Access (L59 Security) - Forms							Roles assigned to User						
Code	Form ID	Title	Role	Security Class	Available Functions	Similar	Isuser	Isadm	mmika	pfadmin	tr Roberts	tnelson	Isu
5	AC001	Activity Group			A,C,D,I,N,P	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS	NO ACCESS	NO ACCESS	NO ACCESS	NO
10	AC002	Calendar			A,C,D,I,N,P	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS	NO ACCESS	NO ACCESS	NO ACCESS	NO
13	AC003	Activity Group Purge Status			C,I,N,P	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS	NO ACCESS	NO ACCESS	NO ACCESS	NO
18	AC011	Mass Activity Copy			+,-,A,C,D,F,I,M,N,P,R,U,V,Z	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS	NO ACCESS	NO ACCESS	NO ACCESS	NO
20	AC012	Additional Parameters			NO FC	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS	NO ACCESS	NO ACCESS	NO ACCESS	NO
22	AC013	Inquire Filter			NO FC	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS	NO ACCESS	NO ACCESS	NO ACCESS	NO
24	AC014	Automatic Activity			A,C,D,I	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS	NO ACCESS	NO ACCESS	NO ACCESS	NO

The user ID will be displayed 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 important considering that a user may have more than one role or security class with access to a form.

	A	B	C	D	E	F	G	H	I	J
	Sys Code	Form ID	Title	Role	Security Class	Available Functions	smiller	lsuser	lsadm	mmitka
+	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	A	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 AC	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 displayed. 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 or hover your mouse pointer over the corresponding cell.

Assigned Roles and Security Classes

To see the Roles and Security Classes 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.



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's on the report. ***This is not necessarily a reflection of all of the Roles and Security Class this form may be assigned to.***

1,2	A	B	C	D	E	F	G	H	I	J
	Sys Code	Form ID	Title	Role	Security Class	Available Functions	smiller	Isuser	Isadm	mnitka
93	AC	AC10.1	Activity			A,C,D,I,N,P	ALL_ACCESS	NO ACCESS	NO ACCESS	ALL_ACCESS
94	AC	AC10.1	Activity	ACAccountant	ACSetup	A,C,D,I,N,P	ALL_ACCESS			ALL_ACCESS
95	AC	AC10.1	Activity	ACAssetManager	ACCapitalization	A,C,D,I,N,P	ALL_ACCESS			ALL_ACCESS
96	AC	AC10.1	Activity	ACExpert	ACCapitalization	A,C,D,I,N,P	ALL_ACCESS			ALL_ACCESS
97	AC	AC10.1	Activity	ACExpert	ACSetup	A,C,D,I,N,P	ALL_ACCESS			ALL_ACCESS
98	AC	AC10.1	Activity	FinSup	ACAnalysis	A,C,D,I,N,P				I
99	AC	AC10.1	Activity	FinSup	ACDataEntry	A,C,D,I,N,P				I

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.

	A	B	C	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:

- 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

Note:

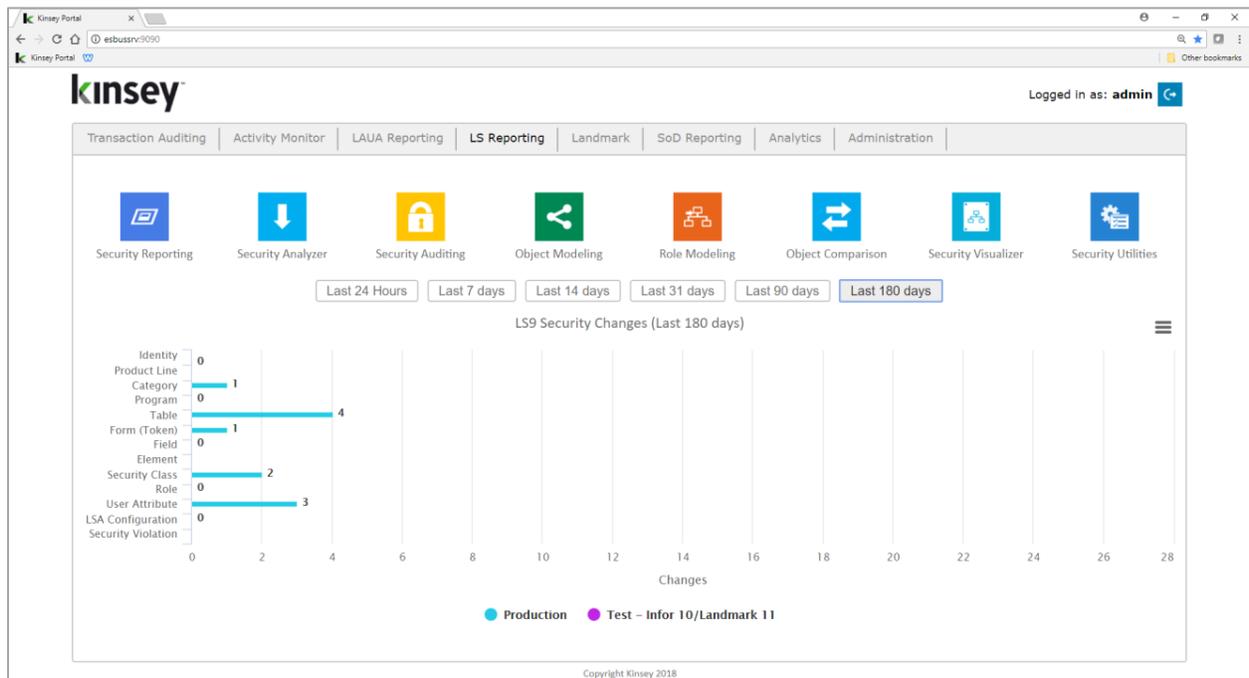
It's important to understand the relationships between various objects in Lawson Security. The values shown in the MS Excel document reflect the exact setting as they appear in Lawson Security, however looking at only one level of security can be misleading. This is because the hierarchy for Token access starts at the System code, then Program and then Token. The Token Excel sheet may indicate that a user has All Access to a form, however if the user does not have access to the program supporting this form then access will be denied. For example, Program AP10 supports Tokens AP10.1 & AP10.2. If Program AP10 is set as NO ACCESS then it doesn't matter what the Token access is set too, access would be denied. This would also be true at the System code level. If System Code AP is restricted then all Programs and Token below the System Code will be restricted.

Additionally "Securable Types" for Programs, Tokens or Tables will override any individual object rule for a user. To indicate this setting the cell containing the user ID is highlighted in the Excel document.

Security Auditing

The Security Audit Report provides a streamlined approach tracking all changes made to your Lawson S3 Security model. This flexible report writer allows you to track critical security changes and setup automatic email notifications.

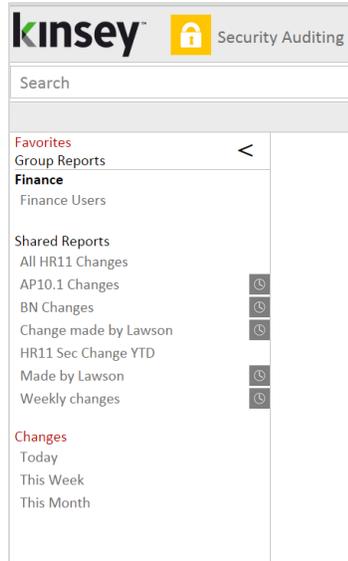
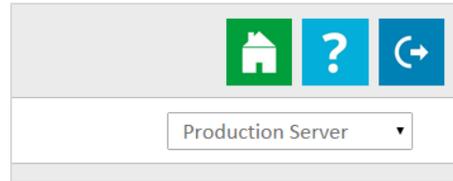
Note: Lawson Security Auditing must be enabled in the Lawson Security Administrator application before using this application.



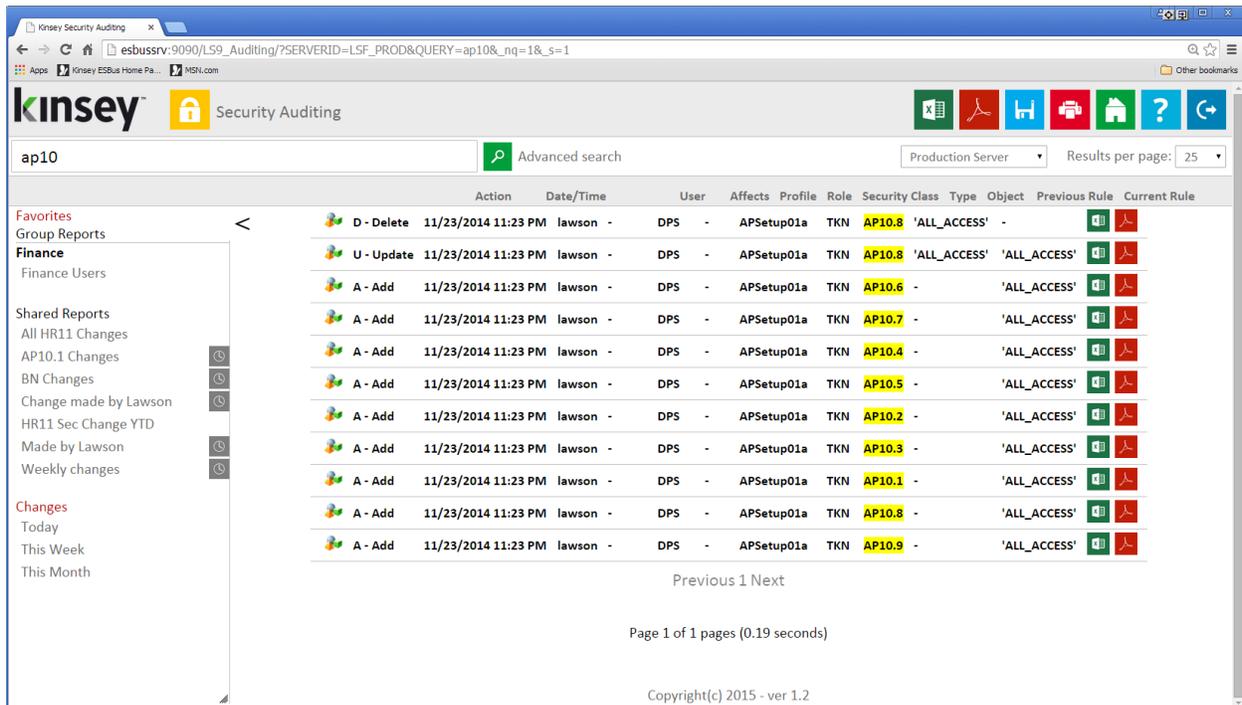
Launch the Security Dashboard and select the Security Auditing icon from the LS Reporting tab.

Security Dashboard User Guide

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



Any saved reports will be displayed in the left navigation pane.



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, Objects 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.

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
 - TFL
 - RMO
 - FLD
 - HDN
 - DTL
- Object
- Value
- Changed To
- Action

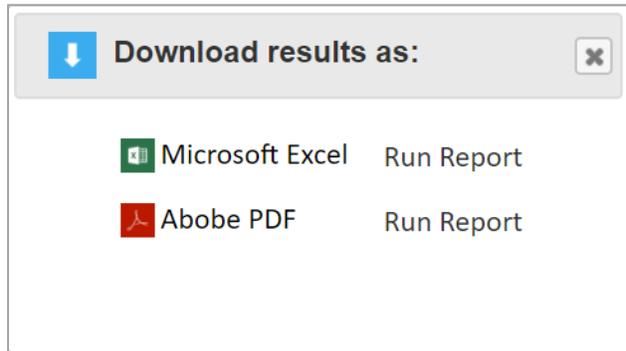
Prompt at Runtime

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

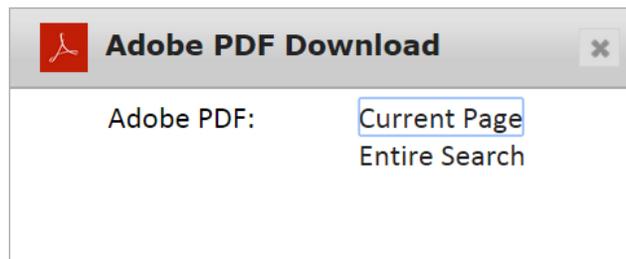
Creating a MS Excel Document

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.



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.

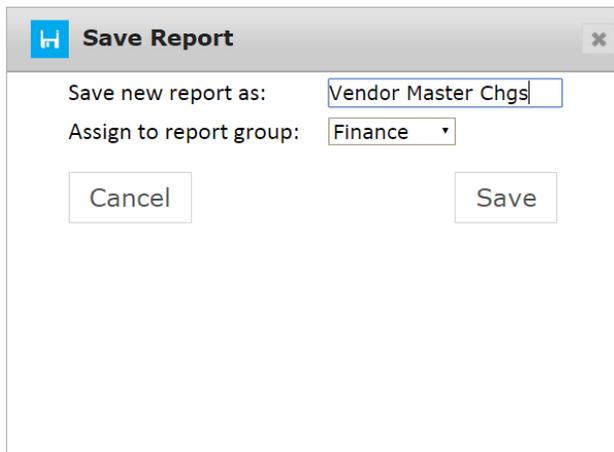


Printing

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 a New Query

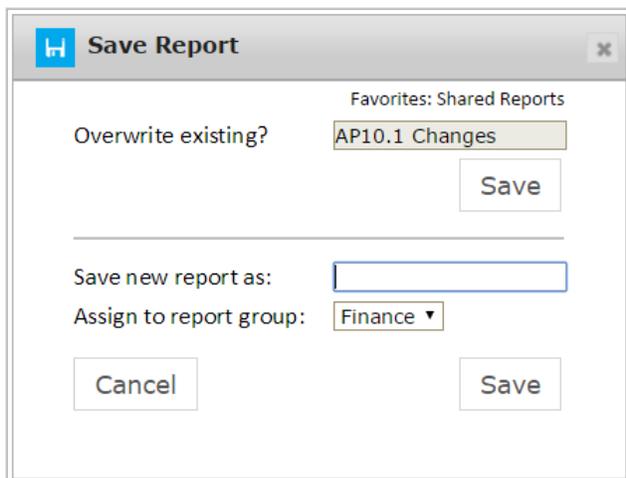
To save a report simply select the Save icon in the top right corner of the screen. Enter a report name and assign the report group for this report. The report group determines which users can view and run a saved report. The report groups are assigned on the administration page under Reporting Groups.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



The image shows a 'Save Report' dialog box with a title bar containing a home icon and a close button. The main area contains two labels: 'Save new report as:' followed by a text input field containing 'Vendor Master Chgs', and 'Assign to report group:' followed by a dropdown menu showing 'Finance'. At the bottom, there are two buttons: 'Cancel' on the left and 'Save' on the right.

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 Guide under Reporting Groups.

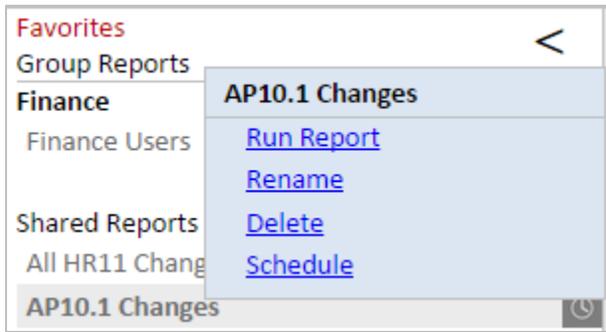


The image shows a 'Save Report' dialog box with a title bar containing a home icon and a close button. The main area is divided into two sections. The top section is titled 'Overwrite existing?' and contains a dropdown menu showing 'AP10.1 Changes' and a 'Save' button. The bottom section is titled 'Save new report as:' and contains a text input field, a dropdown menu showing 'Finance', and a 'Save' button. A 'Cancel' button is located at the bottom left. A 'Favorites: Shared Reports' label is visible at the top right of the dialog.

Scheduling Reports

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

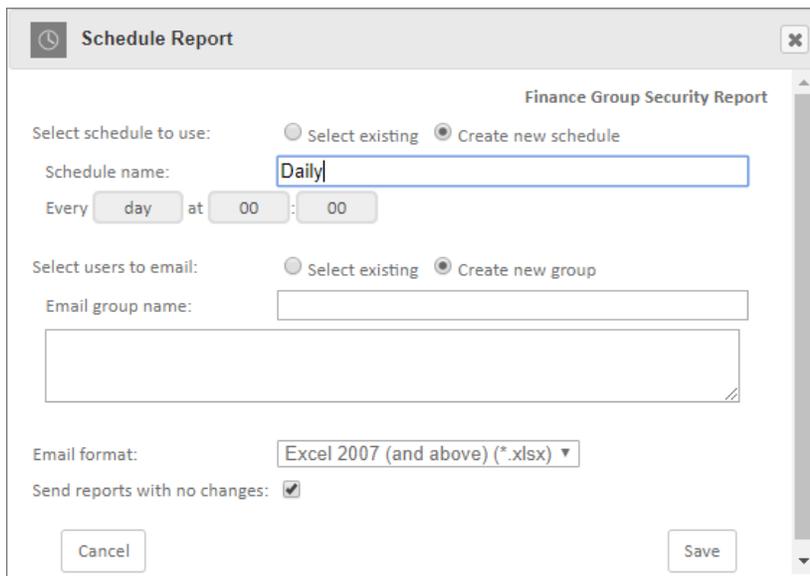
To schedule a report you must first create and save your report. Once the report displays in the left navigation pane right click on the report name and select **Schedule**.



A grey clock icon is displayed next to the report name if a schedule already exist for a report but has not been enabled. A blue clock icon indicates the the schedule is currently enabled.

NOTE: The schedule must be enabled for the schedule to run. To enable a scheduled report refer to the Schedule Reports section of the Administrators Guide.

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. For a new schedule enter a schedule name, frequency and run time.



You can also create or use existing report groups. A report group contains a list of users you want to receive the report. Each user address should be separated by either a comma or a semicolon.

Note: do not insert a return between names in the list.

The screenshot shows a 'Schedule Report' dialog box with the following fields and options:

- Select schedule to use:** Radio buttons for 'Select existing' and 'Create new schedule' (selected).
- Schedule name:** Text input field containing 'Daily'.
- Frequency:** 'Every' dropdown set to 'day', 'at' dropdown set to '20', and '00'.
- Select users to email:** Radio buttons for 'Select existing' and 'Create new group' (selected).
- Email group name:** Text input field containing 'Finance'.
- Email addresses:** Text area containing 'd.kinsey@kinsey.com;m.nitka@kinsey.com'.
- Email format:** Dropdown menu set to 'Excel 2007 (and above) (*.xlsx)'.
- Send reports with no changes:** Checked checkbox.
- Buttons:** 'Cancel' and 'Save' buttons at the bottom.

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 recipient 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.

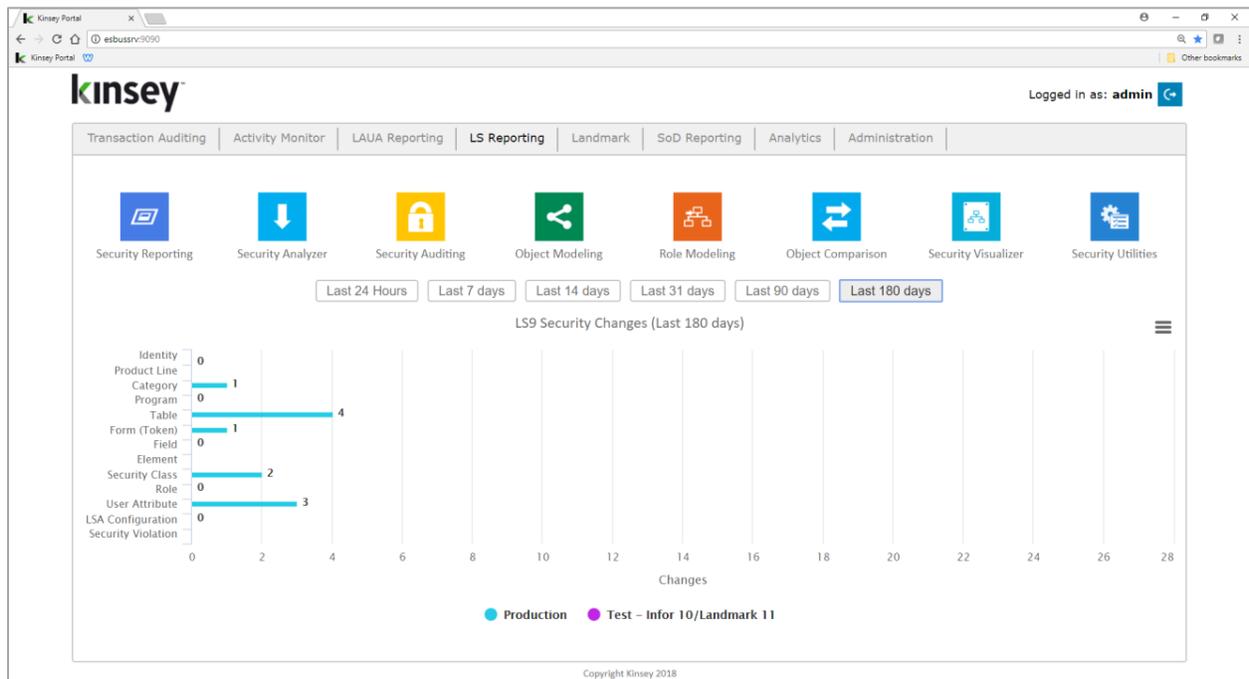
Renaming a Report

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 method of simulating security change to a particular object and project the impact on a users security. The optional security objects are forms, tables and 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.



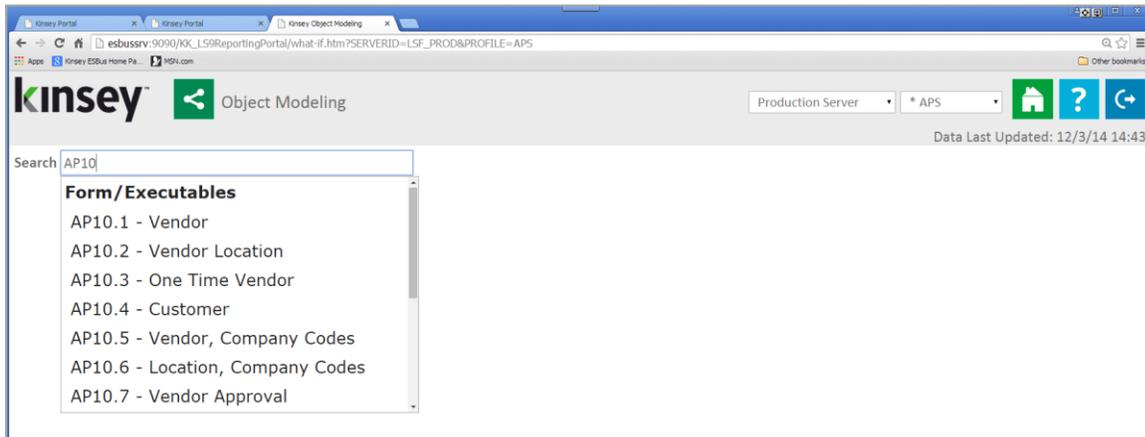
Launch the Security Dashboard and select the Object Modeling icon from the LS Reporting tab.

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



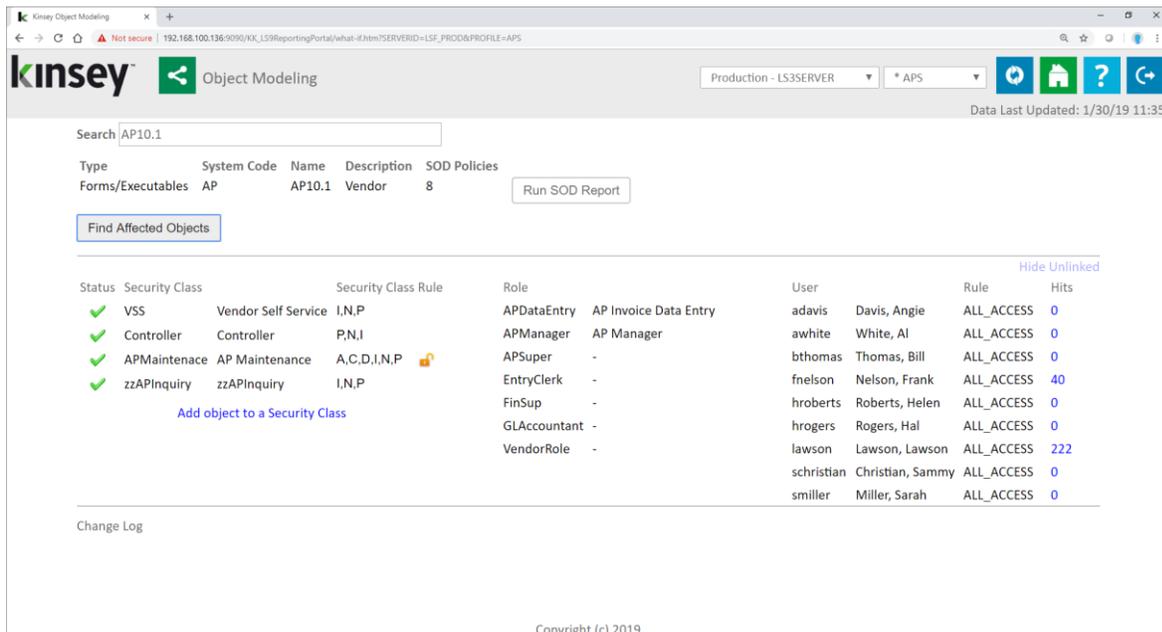
Search

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



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 Security Class Rule indicates that the object has ALL_ACCESS. The function codes are displayed for additional modeling purposes.



The next step is to view the various routes a user might have to access this object. By clicking on the either a Security Class, Role or User the system 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 Security Classes associated with *GLAccountant* that contain the object AP10.1

The screenshot shows the Kinsey Object Modeling interface. At the top, there's a search bar with 'AP10.1' entered. Below it, a table lists object details: Type (Forms/Executables), System Code (AP), Name (AP10.1), Description (Vendor), and SOD Policies (8). A 'Run SOD Report' button is visible. Below this, a table shows 'Object Relationships' for 'User - smiller'. The main table below lists Security Classes and their associated Roles and Users. The user 'smiller' is highlighted in yellow, and a blue line connects her to the role 'GLAccountant'. Another blue line connects 'GLAccountant' to the security class 'zzAPInquiry', which is also highlighted in yellow. A legend at the top right shows 'User - smiller' with a blue line and a 'Hide' link.

Status	Security Class	Security Class Rule	Role	User	Rule	Hits
✓	VSS	Vendor Self Service	I,N,P	adavis	Davis, Angie	ALL_ACCESS 0
✓	Controller	Controller	P,N,I	awhite	White, Al	ALL_ACCESS 0
✓	APMaintenance	AP Maintenance	A,C,D,I,N,P	bthomas	Thomas, Bill	ALL_ACCESS 0
✓	zzAPInquiry	zzAPInquiry	I,N,P	fnelson	Nelson, Frank	ALL_ACCESS 40
			APSuper	hroberts	Roberts, Helen	ALL_ACCESS 0
			EntryClerk	hrogers	Rogers, Hal	ALL_ACCESS 0
			FinSup	lawson	Lawson, Lawson	ALL_ACCESS 222
			GLAccountant	schristian	Christian, Sammy	ALL_ACCESS 0
			VendorRole	smiller	Miller, Sarah	ALL_ACCESS 0

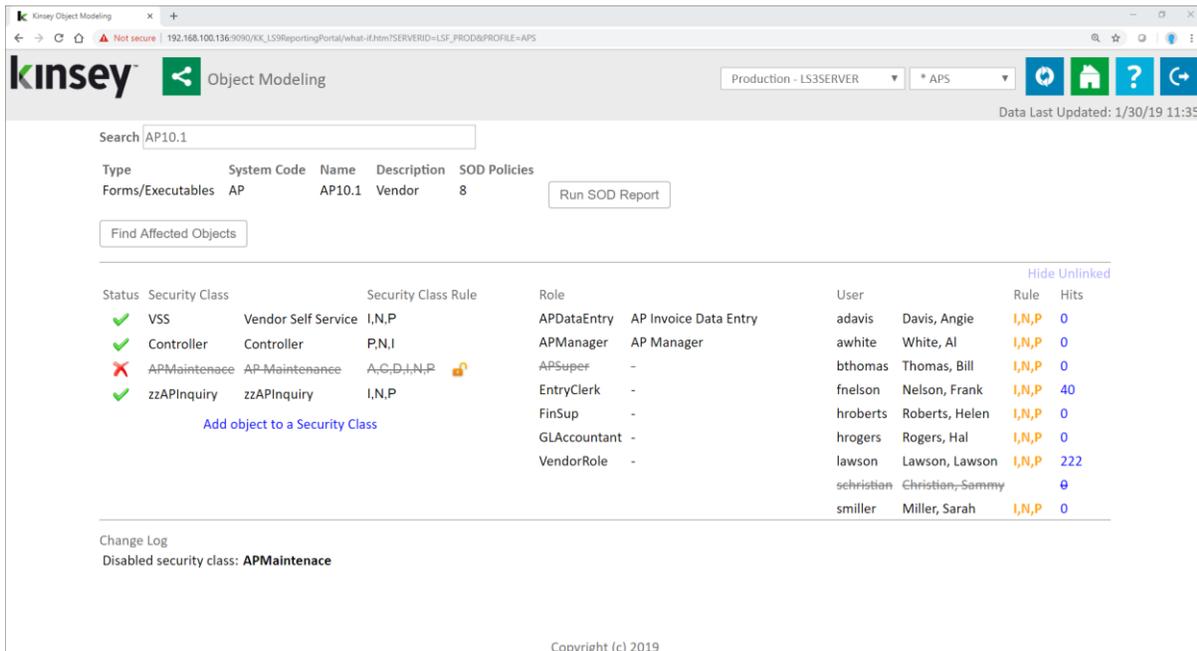
Similarly you can click on the Security Class *APSetup* and see the associated Roles and Users associated with the Security Class or select a Role and map to the Security Class and Users associated with the Role. You can cancel the mapping by clicking on the Hide link option on the legend.

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

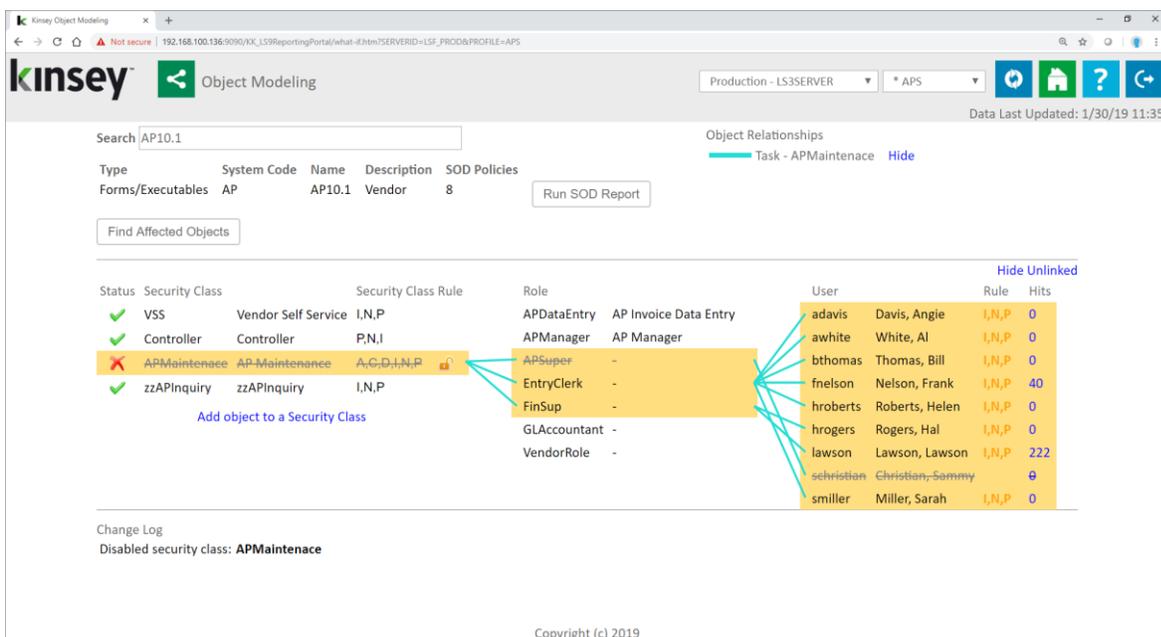
1. Remove the object from an existing Security Class
2. Add the object to a new Security Class
3. Change a Security Class rule
4. Generate Security Reports based on the object selected
5. View potential Segregation of Duties violations.

Removing an Object Assignment from a Existing Security Class

To visually see the affect of removing an object from a Security Class simply click on the green check mark left of the Security Class list. If the access rule for a User changes the new rule will be displayed in orange to the right of the users name.



Clicking on the Security Class title will display a mapping of all users connected to the Security Class.



To see why the users access rule has changed click on the user ID. The application will map the user to their available Security Classes. In the example below the user hroberts also had access to AP10.1 through the zzAPInquiry Security Class and thus receives Inquiry access. So deleting AP10.1 from Security Classes APMaintenance won't remove complete access for hroberts because Inquire access is provided through a different Security Class.

Search AP10.1

Object Relationships
 Task - APMaintenance Hide
 User - hroberts Hide

Type	System Code	Name	Description	SOD Policies	Run SOD Report
Forms/Executables	AP	AP10.1	Vendor	8	Run SOD Report

Find Affected Objects

Status	Security Class	Security Class Rule	Role	User	Rule	Hits
✓	VSS	Vendor Self Service	I,N,P	adavis Davis, Angie	I,N,P	0
✓	Controller	Controller	P,N,I	awhite White, Al	I,N,P	0
✗	APMaintenance	AP-Maintenance	A,C,D,I,N,P	bthomas Thomas, Bill	I,N,P	0
✓	zzAPInquiry	zzAPInquiry	I,N,P	fnelson Nelson, Frank	I,N,P	40
				hroberts Roberts, Helen	I,N,P	0
				hrogers Rogers, Hal	I,N,P	0
				lawson Lawson, Lawson	I,N,P	222
				schristian Christian, Sammy		
				smiller Miller, Sarah	I,N,P	0

Change Log
 Disabled security class: **APMaintenance**

Copyright (c) 2019

Adding an Object to a New Security Class

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

Add object (AP10.1) to the Task:

Cancel

- ACCapitalization - Activity Capitalization 1
- APAnalysis - Accounts Payable Analysis
- APPLSS - Applicant Self Service
- APPLSSINQ - Test Addition Inquire
- APProcessing - Accounts Payable Processing Screens
- APSetup - Accounts Payable Setup

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

Adding form AP10.1 to *APAnalysis* could produce multiple results including the addition of Roles and Users displaying on the map or changes to a Rule for affected uses.

Search: AP10.1

Object Relationships: Task - APAnalysis

Type	System Code	Name	Description	SOD Policies
Forms/Executables	AP	AP10.1	Vendor	8

Find Affected Objects

Status	Security Class	Security Class Rule	Role	User	Rule	Hits
✓	VSS	Vendor Self Service	I,N,P	adavis	Davis, Angie	ALL_ACCESS 0
✓	Controller	Controller	P,N,I	awhite	White, Al	ALL_ACCESS 0
✓	APMaintenance	AP Maintenance	A,C,D,I,N,P	bthomas	Thomas, Bill	ALL_ACCESS 0
✓	zzAPInquiry	zzAPInquiry	I,N,P	fnelson	Nelson, Frank	ALL_ACCESS 40
✓	APAnalysis	Accounts Payable Analysis	A,C,D,I,N,P	hroberts	Roberts, Helen	ALL_ACCESS 0
			GLAccountant	hrogers	Rogers, Hal	ALL_ACCESS 0
			VendorRole	lawson	Lawson, Lawson	ALL_ACCESS 222
			APInquiry	schristian	Christian, Sammy	ALL_ACCESS 0
				smiller	Miller, Sarah	ALL_ACCESS 0

Change Log
 Disabled security class: **APMaintenance**
 Added security class: **APAnalysis**
 Enabled security class: **APMaintenance**

Changing a Forms Function Code Rule

This option provides the ability to see the impact of changing a rule on a Form for a specific Security Class. In the example below the mapping indicates that 9 users have ALL_ACCESS to form AP10.1 via the *APMaintenance* Security Class.

Search: AP10.1

Object Relationships: Task - APMaintenance

Type	System Code	Name	Description	SOD Policies
Forms/Executables	AP	AP10.1	Vendor	8

Find Affected Objects

Status	Security Class	Security Class Rule	Role	User	Rule	Hits
✓	VSS	Vendor Self Service	I,N,P	adavis	Davis, Angie	ALL_ACCESS 0
✓	Controller	Controller	P,N,I	awhite	White, Al	ALL_ACCESS 0
✓	APMaintenance	AP Maintenance	A,C,D,I,N,P	bthomas	Thomas, Bill	ALL_ACCESS 0
✓	zzAPInquiry	zzAPInquiry	I,N,P	fnelson	Nelson, Frank	ALL_ACCESS 40
✓	APAnalysis	Accounts Payable Analysis	A,C,D,I,N,P	hroberts	Roberts, Helen	ALL_ACCESS 0
			APSuper	hrogers	Rogers, Hal	ALL_ACCESS 0
			EntryClerk	lawson	Lawson, Lawson	ALL_ACCESS 222
			FinSup	schristian	Christian, Sammy	ALL_ACCESS 0
			APInquiry	smiller	Miller, Sarah	ALL_ACCESS 0

Change Log
 Disabled security class: **APMaintenance**
 Added security class: **APAnalysis**
 Enabled security class: **APMaintenance**

To see the impact of changing the current rule simply click on the rule and a box will appear.

Status	Security Class	Security Class Rule
✓	VSS	Vendor Self Service I,N,P
✓	Controller	Controller P,N,I
✓	APMaintenance	AP Maintenance A,C,D,I,N,P
✓	zzAPInquiry	zzAPInquiry I,N,P

At this point you can change the level of access and if the user is impacted by this change their new security rules will be displayed in orange once you exit the field.

The screenshot shows the Kinsey Object Modeling application. The main window displays a table of security classes and a list of users. The 'APMaintenance' security class rule is highlighted in orange, and the 'A,I,N,P' rule is selected. A 'Change Log' section at the bottom indicates the security class was changed from 'A,C,D,I,N,P' to 'A,I,N,P'.

Status	Security Class	Security Class Rule	Role	User	Rule	Hits
✓	VSS	Vendor Self Service	I,N,P	adavis Davis, Angie	A,I,N,P	0
✓	Controller	Controller	P,N,I	awhite White, Al	A,I,N,P	0
✓	APMaintenance	AP Maintenance	A,I,N,P	bthomas Thomas, Bill	A,I,N,P	0
✓	zzAPInquiry	zzAPInquiry	I,N,P	fnelson Nelson, Frank	A,I,N,P	40
				hroberts Roberts, Helen	A,I,N,P	0
				hrogers Rogers, Hal	A,I,N,P	0
				lawson Lawson, Lawson	A,I,N,P	222
				schristian Christian, Sammy	A,I,N,P	0
				smiller Miller, Sarah	A,I,N,P	0

Change Log
 Changed security class: **APMaintenance** from A,C,D,I,N,P to A,I,N,P

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

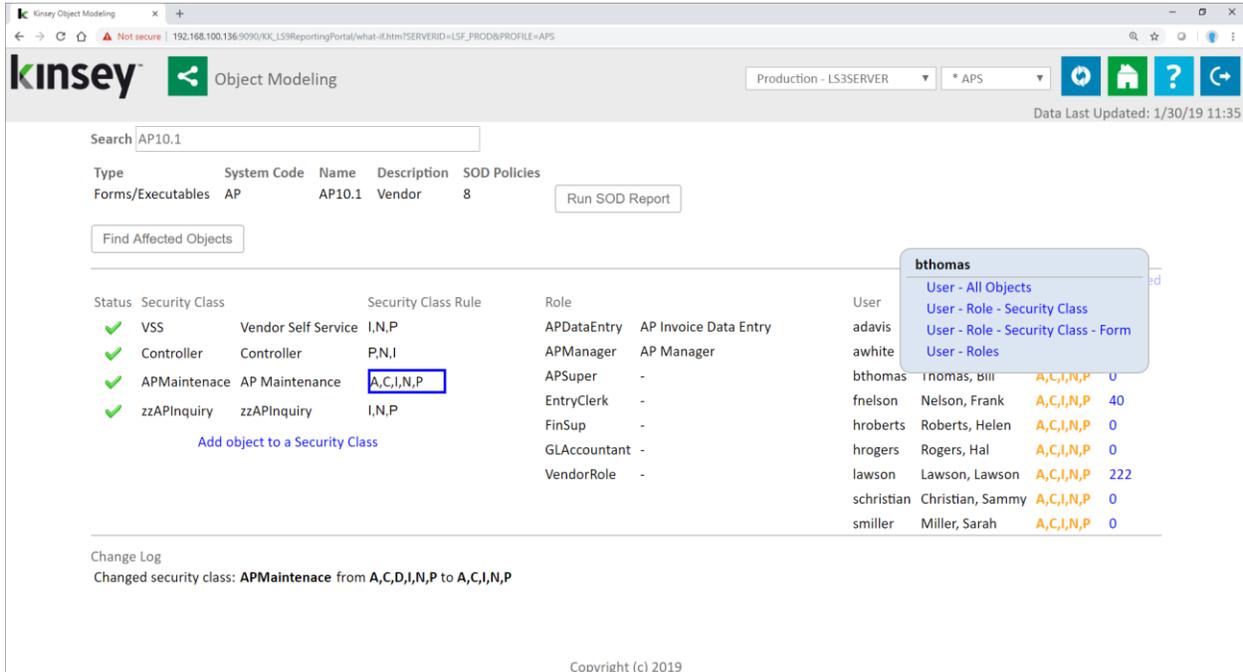
Note: The application will display the "least restrictive" access to the object you are working with. For example, if a user is assigned a Role that provides Inquiry only access and another Role that provides ALL_ACCESS the users access will be displayed as ALL_ACCESS (least restrictive)

Additional Rule options that will be resolved correctly are:

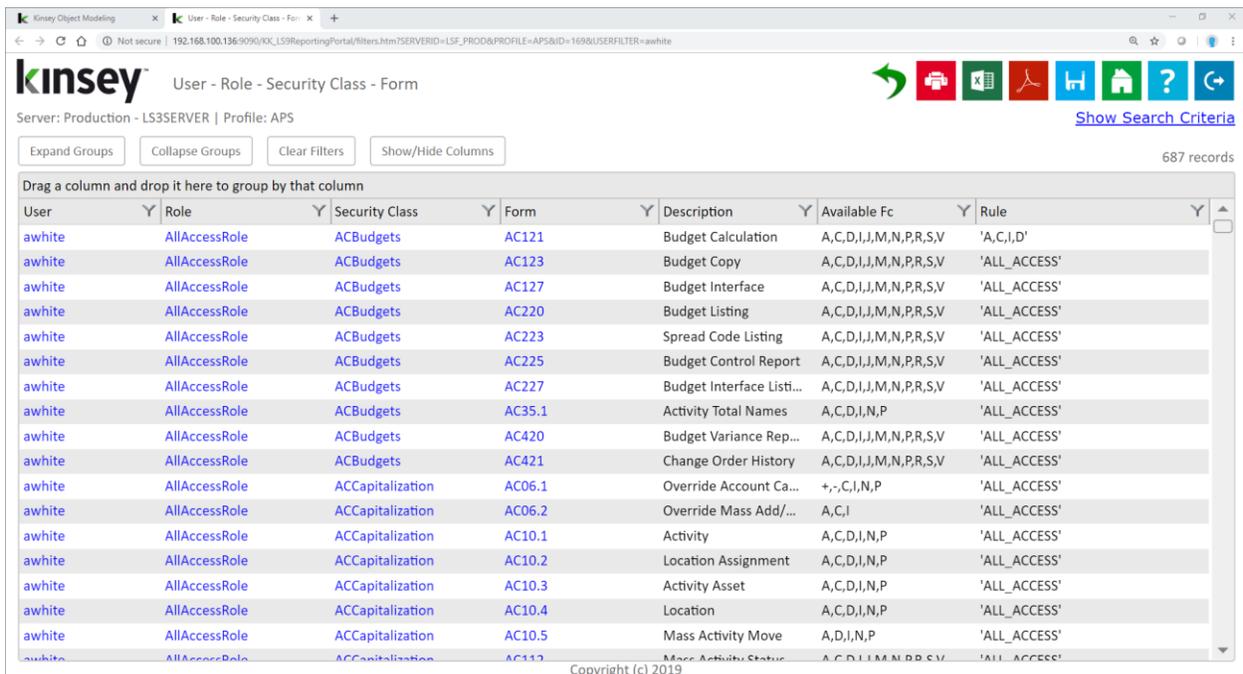
- ALL_ACCESS
- ALL_INQUIRY
- ALL_DELETE
- ALL_ADD
- NO_ACCESS

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.



In this example you can view the User Security by right clicking on the User ID



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 Security Class assignment 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.

The screenshot shows the Kinsey Object Modeling interface. At the top, there's a search bar with 'AP10.1' and a 'Run SOD Report' button. Below, a table lists Security Class Rules. The 'APMaintenance' rule is highlighted in orange, indicating it's affected. A list of users is shown to the right, with lines connecting them to the affected rule. The 'Hits' column shows the number of violations for each user.

Status	Security Class	System Code	Name	Description	SOD Policies	Role	User	Rule	Hits
✓	VSS	Vendor Self Service	I,N,P			APDataEntry	adavis Davis, Angie	A,I,N,P	0
✓	Controller	Controller	P,N,I			APManager	awhite White, Al	A,I,N,P	0
✓	APMaintenance	AP Maintenance	A,I,N,P			APSuper	bthomas Thomas, Bill	A,I,N,P	0
✓	zzAPInquiry	zzAPInquiry	I,N,P			EntryClerk	fnelson Nelson, Frank	A,I,N,P	40
						FinSup	hroberts Roberts, Helen	A,I,N,P	0
						GLAccountant	hrogers Rogers, Hal	A,I,N,P	0
						VendorRole	lawson Lawson, Lawson	A,I,N,P	222
							schristian Christian, Sammy	A,I,N,P	0
							smiller Miller, Sarah	A,I,N,P	0

Change Log
 Changed security class: **APMaintenance** from A,C,D,I,N,P to A,I,N,P

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

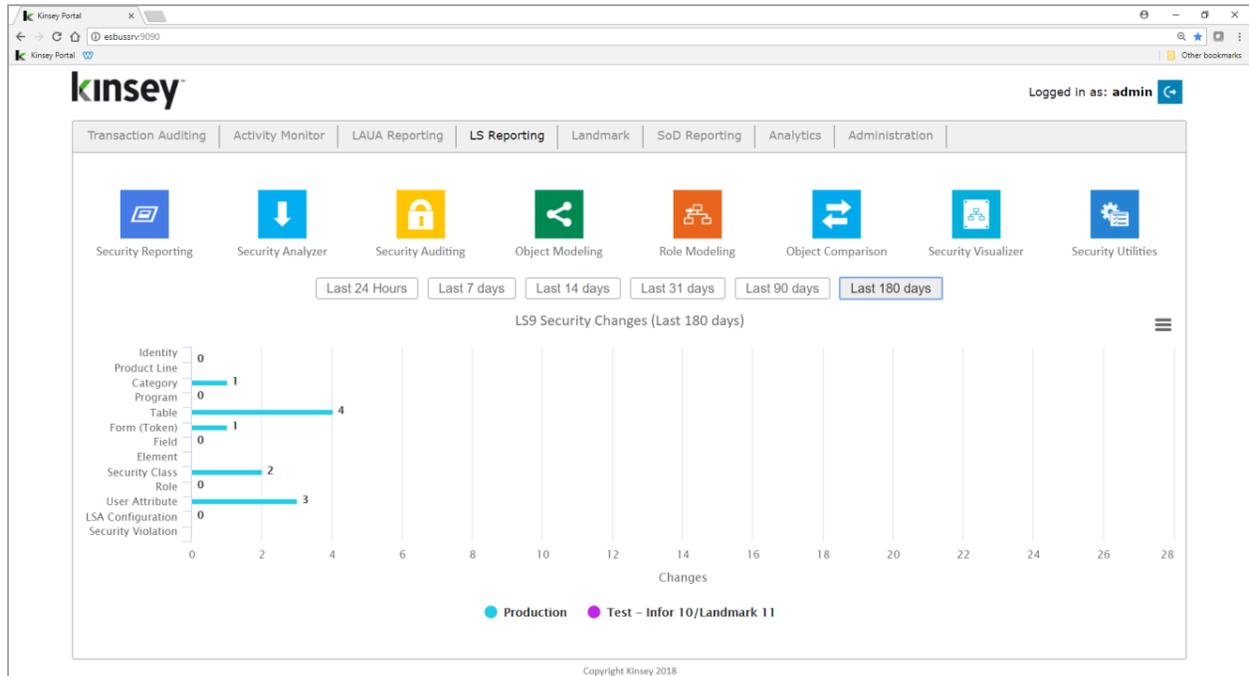
Select the SOD Reporting link. Once the report is finished the application will display the following options.

-  SOD Report Sorted by User
-  SOD Report Sorted by Policy
-  SOD Report by Role Group
-  SOD Report by Role Group

Role Modeling

The Role Modeling application provides a way to simulate the impact on security of changing User Role assignments 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 Profile 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.

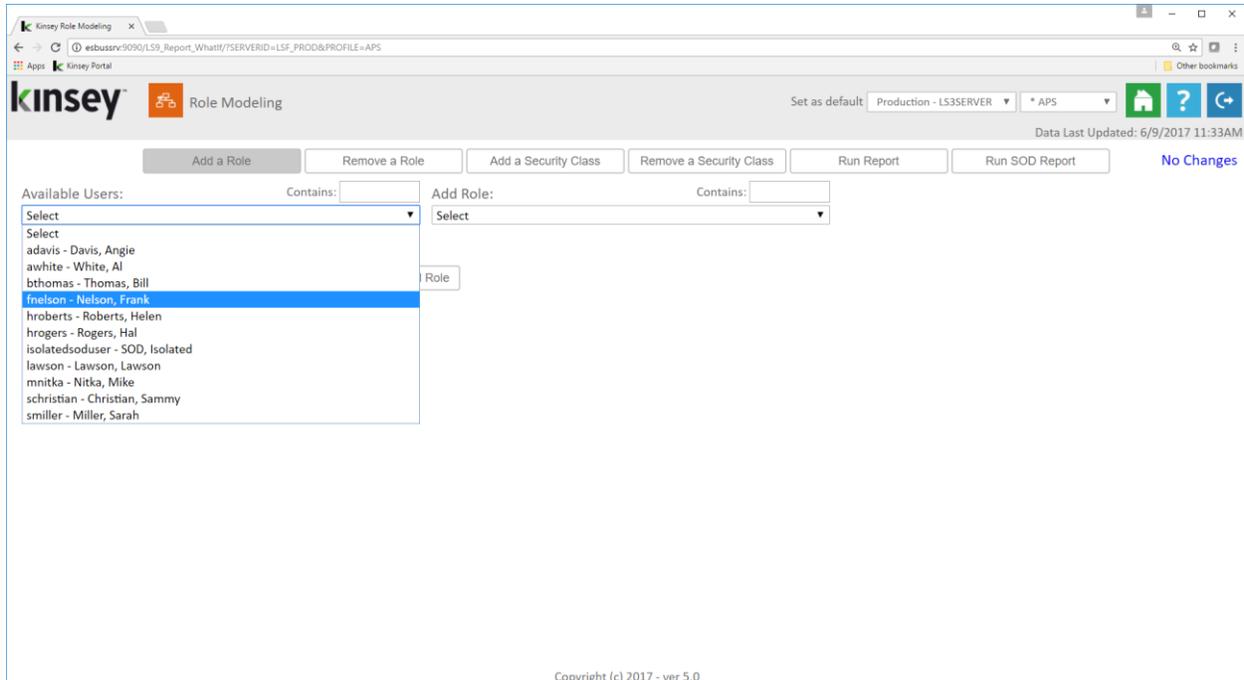
The following modeling options are available:

- 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

Changing Role Assignments

The option of adding a new Role or removing an existing Role are very similar. This documentation guides you through the process of adding a new Role to a User. You can simulate adding or removing multiple roles prior to running a security simulation report.

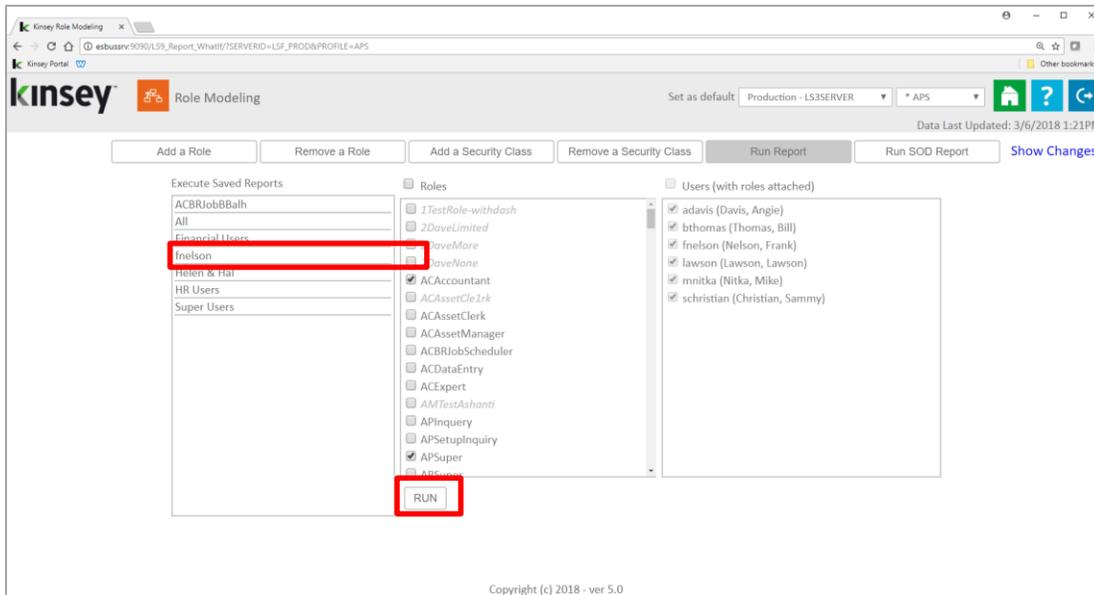
On the Add a Role tab select a user from the dropdown list. The application will display the Roles currently assigned to the user.



Using the Add Role dropdown select the Role you would like to add and click on the Add Role button. A list of your current selection is displayed in the top right corner of the screen. There is no limit to the number of changes you can simulate 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.

Once you have finished your selections click on the Run Report tab. The application will launch the LS Security Analyzer reporting screen. From there you can run a pre-saved report or select the RUN button to generate a report based on the simulation criteria. Running a report based on the simulation criteria will include all users assigned to any role selected in the simulation. This is true even if you are simply adding a role to a user. Any other users that share that same role will be included on the report.

Security Dashboard User Guide



By selecting fnelson from the saved report list the Excel document will only include fnelson results, however if you are not using a saved a report you can select RUN to generate an report showing all users attached to the role you are simulating. The screen shot below are the results of the fnelson report. Had the RUN button been selected instead, all of the users in the User window would have been included on the report.

The color of the cell is an indication of the level of change to a user's access.

Black
Indicates no change

Red
Object access was removed

Green
Object access was granted

Blue
Object access has changed

Sys Code	Form ID	Title	Role	Security Class	Available Functions	Users
AC	AC00.1	Activity Group			A,C,D,I,N,P	I,N,P
AC	AC00.2	Calendar			A,C,D,I,N,P	I,TIME_RULE
AC	AC00.3	Activity Group Purge Status			C,I,N,P	I
AC	AC01.1	Mass Activity Copy			+,-,A,C,D,F,I,M,N,P,R,U,V	NO_ACCESS
AC	AC01.2	Additional Parameters			NO FC	NO_ACCESS
AC	AC01.3	Inquire Filter			NO FC	NO_ACCESS
AC	AC01.4	Automatic Activity			A,C,D,I	NO_ACCESS
AC	AC01.5	Automatic Level			A,C,D,I	NO_ACCESS
AC	AC02.1	Status			+,-,A,C,I	I
AC	AC03.1	Resource			A,C,D,I,N,P	I
AC	AC03.2	AC Person Assignment			+,-,A,C,I,N,P	I
AC	AC03.3	HR Employee Assignment			+,-,A,C,I,N,P	I
AC	AC03.4	Vendor Assignment			+,-,A,C,I,N,P	I
AC	AC03.5	Asset Assignment			+,-,A,C,I,N,P	I
AC	AC03.6	Equipment Assignment			+,-,A,C,I,N,P	I
AC	AC03.7	Role Assignment			+,-,A,C,D,I,N,P	I
AC	AC03.8	Roles			+,-,A,C,I	I
AC	AC03.9	Resource Account			C,I	I
AC	AC04.1	GL Code			+,-,A,C,I	I
AC	AC05.1	Account Categories			NO FC	I
AC	AC06.1	Override Account Categories			+,-,C,I,N,P	I
AC	AC06.2	Override Mass Add/Change			A,C,I	I

SOD Validation

Once you have made the required changes you can cross check the new security settings against your SOD policies. You have the option of running a saved SOD report or creating a new report.

Navigation Menu (Favorites):

- ACAccountant
- Asset Management
- Cash Mgmt
- Closing Policies
- Entry Clerk
- Financial policies
- Landmark Policies
- Payables
- Payroll
- Receivables
- Receiving and Requisitions

Report Configuration:

- Report Type: LS * APS
- Category:
 - ASSET MANAGEMENT
 - CASH MANAGEMENT
 - CLOSING
 - INVENTORY
 - LANDMARK
 - ORDER ENTRY
 - PAYABLES
 - PAYROLL
 - PURCHASING
 - RECEIVABLES
- Rating: All Star Ratings
- Form Filter:

ASSET MANAGEMENT Policies:

- 1** Initiate Disposal of Fixed Assets conflicts with Reconcile Fixed Assets Subsidiary Ledger to General Ledger. One person should not have responsibility over both the access to assets and the responsibility for maintaining the accountability for such assets. (10-11)

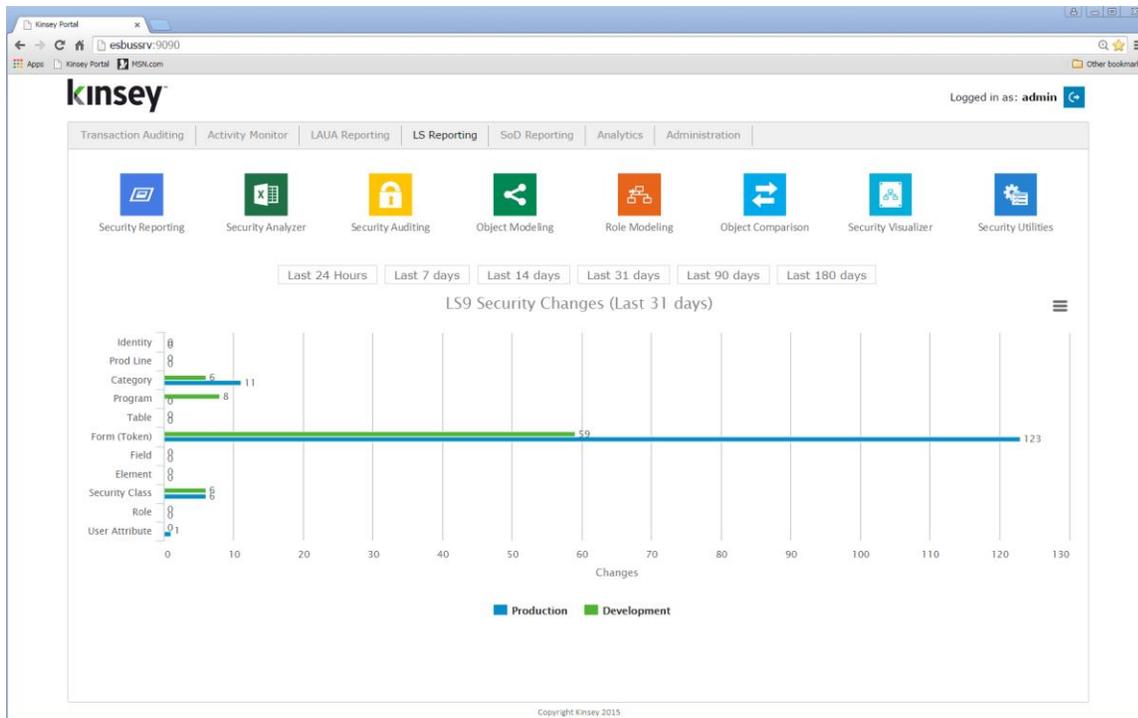
[Show/Hide Policy Details](#) ★★☆☆☆☆
- 3** Initiate Disposal of Fixed Assets conflicts with Edit Fixed Asset Master File. If one individual has responsibility for more than one of these functions, that individual could misappropriate assets and conceal the misappropriation. (10-14)

[Show/Hide Policy Details](#) ★★☆☆☆☆

Copyright (c) 2019 - ver 5.0

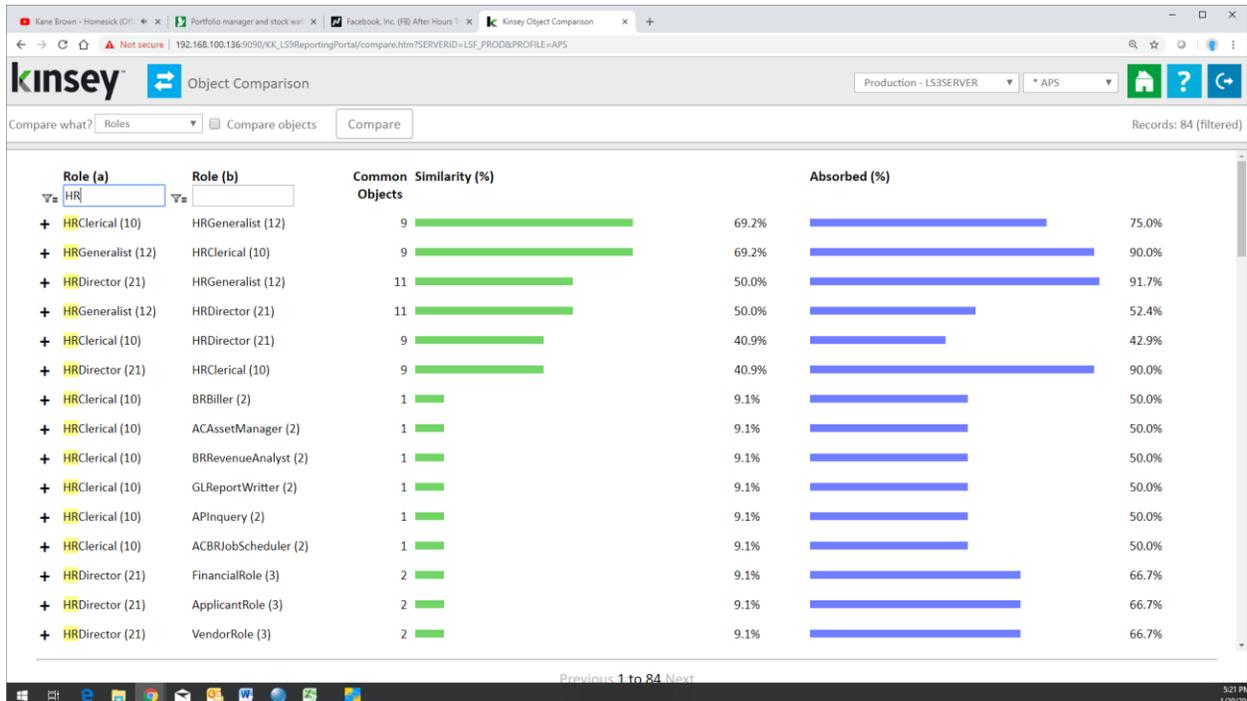
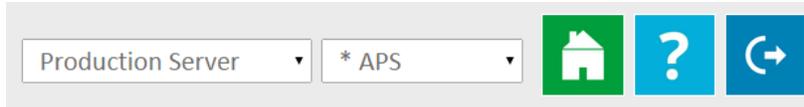
Object Comparison

The Object Comparison application allows you to check for redundancies in your security model. By comparing every Role to every other Role or every Security Class to every other Security Class 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 high percentage.



Launch the Security Dashboard from your Windows browser and from the LS Reporting tab and select the Object Comparison icon.

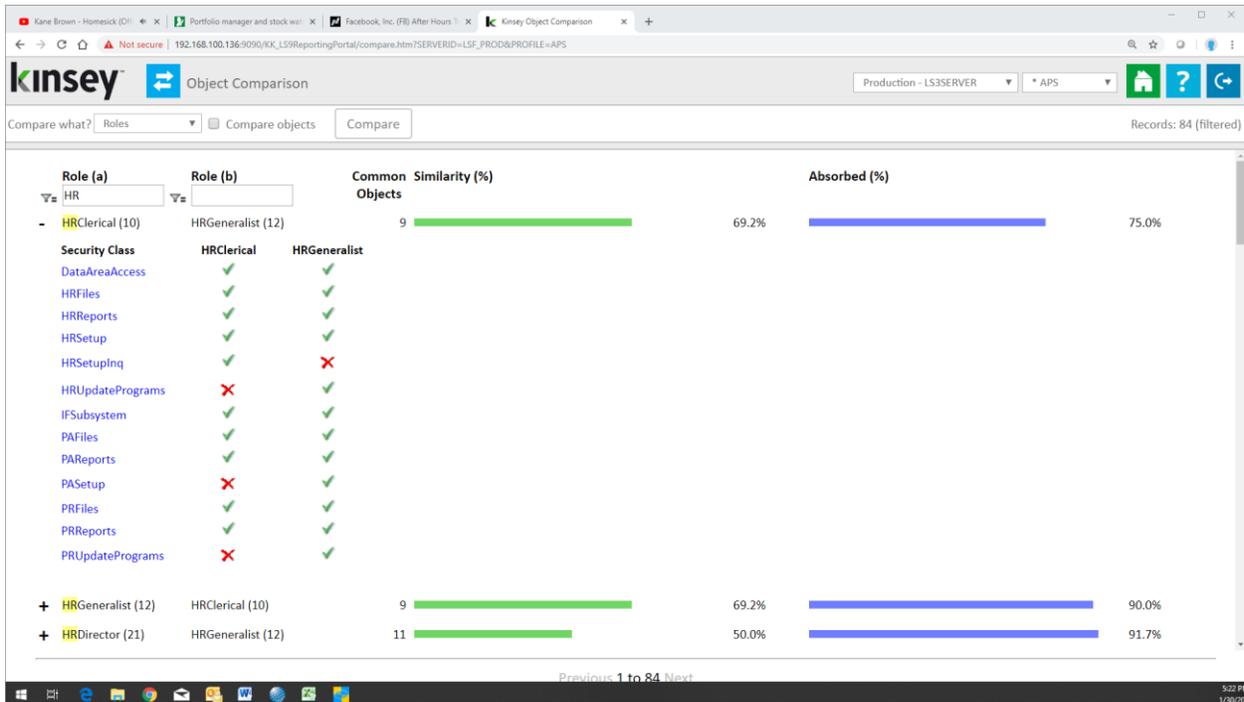
Start by selecting the server and security profile you want to work with in in the top right corner of the screen.



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

Comparing Role-Security Class 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-Security Classe assignments are and where one Role could completely absorb another Role.



In this example you can see that the Roles *HR Clerical* and *HR Generalist* are 69.2% similar (green graph) By clicking on the plus sign left of the Role you can see how the Roles differ in their Security Class assignments. You can also drill to the the security reports for more information on a specific Security Class by right clicking on the Security Class name.

The absorption graph (blue) indicates how much one Role can completely absorb another Role.

Comparing Role-Security Class 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 the access rules for forms, categories, programs and tables.

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.

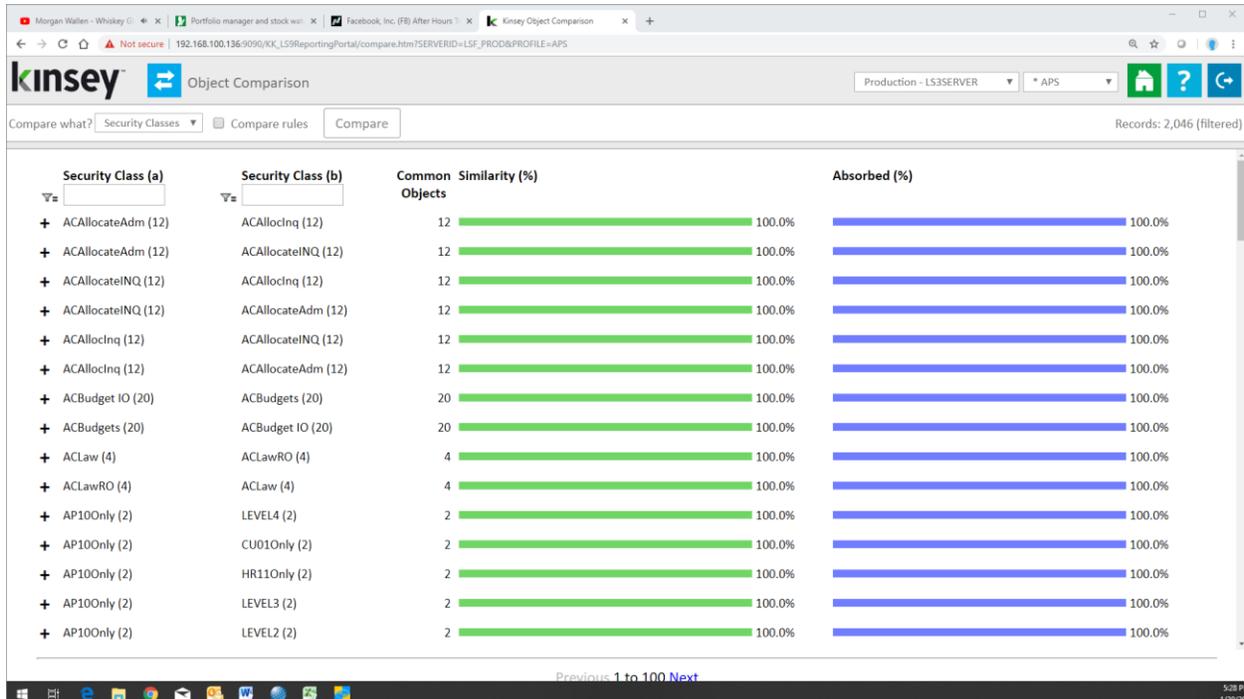
Role	Object	Access	Comparison
PGM PA80	HRGeneralist PAMSetup	'ALL_ACCESS'	-
PGM PA81	HRGeneralist PAMSetup	'ALL_ACCESS'	-
PGM PA90	HRGeneralist PAMSetup	'ALL_ACCESS'	-
PGM PA91	HRGeneralist PAMSetup	'ALL_ACCESS'	-
PGM PA93	HRGeneralist PAMSetup	'ALL_ACCESS'	-
PGM PA94	HRGeneralist PAMSetup	'ALL_ACCESS'	-
PGM PA95	HRGeneralist PAMSetup	'ALL_ACCESS'	-
PGM PA96	HRGeneralist PAMSetup	'ALL_ACCESS'	-
TKN HR00.1	HRGeneralist HRSetup	'ALL_ACCESS'	HR Clerical HRSetupInq 'I,N,P'
TKN HR00.2	HRGeneralist HRSetup	'ALL_ACCESS'	HR Clerical HRSetupInq 'I,N,P,+,-'
TKN HR00.3	HRGeneralist HRSetup	'ALL_ACCESS'	HR Clerical HRSetupInq 'I,N,P,+,-'
TKN HR01.1	HRGeneralist HRSetup	'ALL_ACCESS'	HR Clerical HRSetupInq 'I,N,P'
TKN HR02.1	HRGeneralist HRSetup	'ALL_ACCESS'	HR Clerical HRSetupInq 'I,+,-'
TKN HR10.1	HRGeneralist HRSetup	'ALL_ACCESS'	HR Clerical HRSetupInq 'I,+,-'
TKN HR105	HRGeneralist HRUpdatePrograms	'ALL_ACCESS'	-
TKN HR11.1	HRGeneralist HRSetup	'ALL_ACCESS'	HR Clerical HRSetupInq '+,-,I,N,P,M'
TKN HR11.2	HRGeneralist HRSetup	'ALL_ACCESS'	HR Clerical HRSetupInq 'I'
TKN HR11.3	HRGeneralist HRSetup	'ALL_ACCESS'	HR Clerical HRSetupInq 'NO_ACCESS'
TKN HR125	HRGeneralist HRUpdatePrograms	'ALL_ACCESS'	-
TKN HR130	HRGeneralist HRUpdatePrograms	'ALL_ACCESS'	-
TKN HR155	HRGeneralist HRUpdatePrograms	'ALL_ACCESS'	-
TKN HR16.4	-	-	HR Clerical HRSetupInq 'ALL_ACCESS'
TKN HR170	HRGeneralist HRUpdatePrograms	'ALL_ACCESS'	-
TKN HR18.1	-	-	HR Clerical HRSetupInq 'ALL_ACCESS'

In this example you can see that the Roles *HR Clerical* and *HR Generalist* are now 72.91 similar (green graph) in stead of 69.2% as reflected at the Role-Security Class level. By clicking on the plus sign left of the Role you can see how the Roles differ in their assignments. Only the differences are displayed. To get a full view of all objects in a Role or Security Class you can drill to the security reports.

Blue highlights reflect rule differences where as pink highlights objects that are not included in one Role or the other.

Comparing Security Class Assignments

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



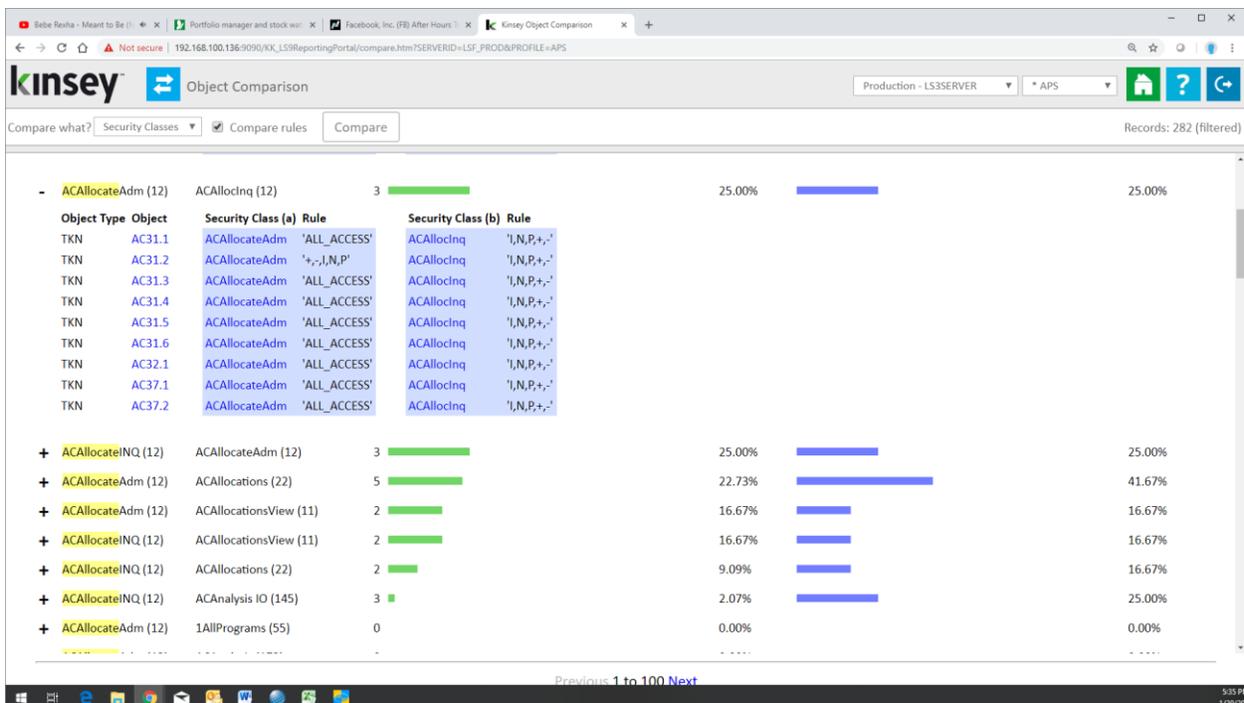
In this example you can see that the Security Class *ACAllocateAdm* and *ACAllocInq* are 100% similar (green graph) at the Security Class-Object level. This level of reporting does not take the rule into account, only the object assignment. By clicking on the plus sign left of the Security Class you can see how the Security Classes 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 absorption graph (blue) indicates how much one Security Class can completely absorb another Security Class. In the example above you can see that all of the Objects assigned to the *ACAllocInq* Security Class are also assigned to the *ACAllocateAdm* Security Class. This is not necessarily an indication that you can eliminate either Security Class. At this point no comparison has been done at the Rule level.

Comparing SecurityAssignments 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 the rules for categories, programs, tables and tokens are assigned to a Security Class.

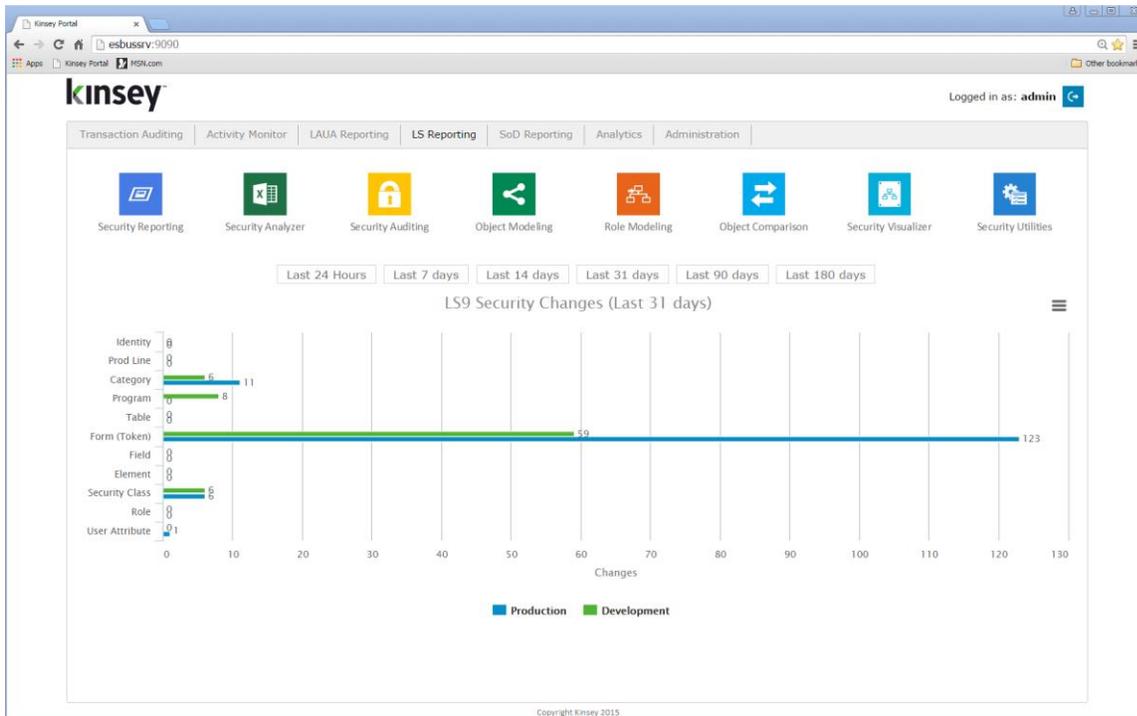
Once you have selected the server and profile select Security Classes from the ‘Compare What?’ dropdown window, select the Compare Objects checkbox and then click on the Compare button. The application will compare every Security Class to every other Security Class. The graph will reflect how similar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



In this example you can see that the Security Class *ACAllocateAdm* and *ACAllocateInq* now only 25% similar (green graph) in stead of 100% as reflected at the Security Class-Object level. By clicking on the plus sign left of the Security Class you can see how the Security Classes differ in their assignments. Only the differences are displayed when a Class is expanded. You can drill to the the security reports for more information on a specific Class by right clicking on the Class ID.

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 level. Additionally you can assign Roles to Users or Security Class to Roles and upload the changes to LS security provide you have valid credentials.

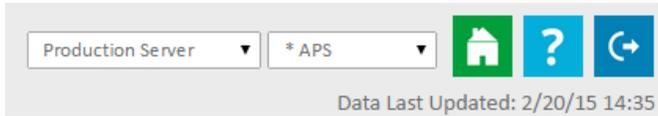


Launch

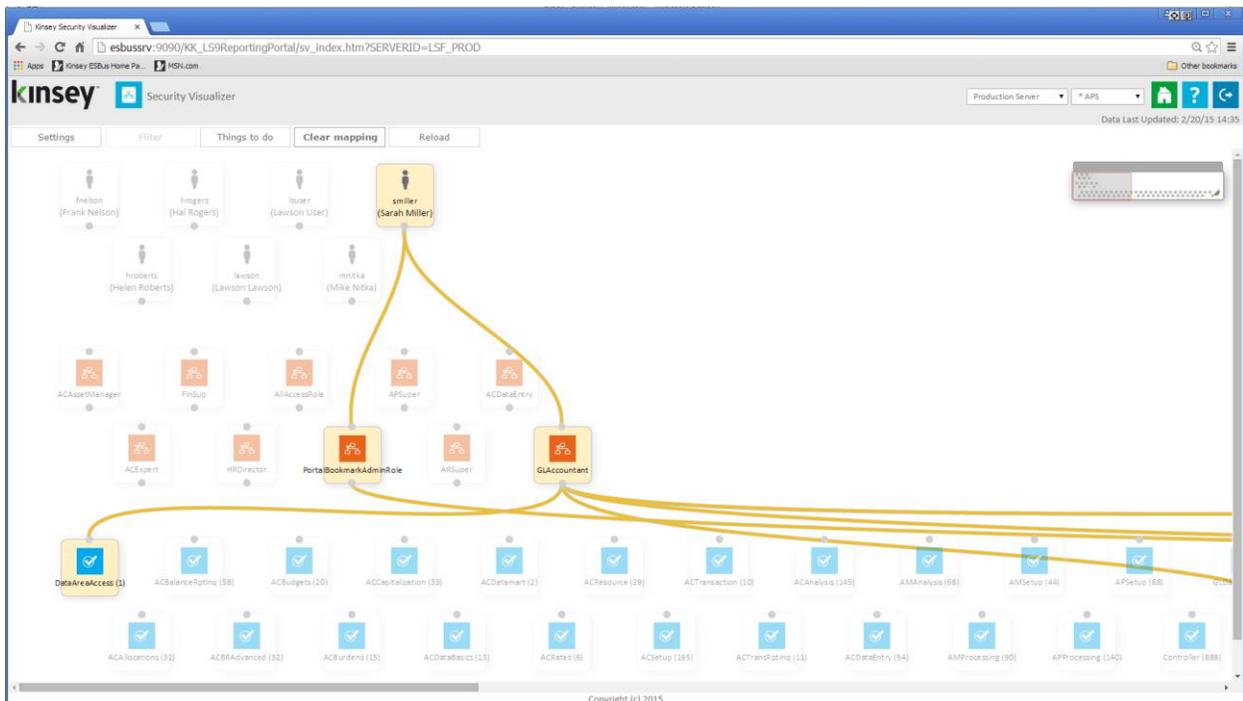
Launch the Dashboard from your Windows browser and from the LS Reporting tab and select the Security Visualizer icon.

Displaying a User Map

Start by selecting the server and security profile you want to access in the top right corner of the screen.



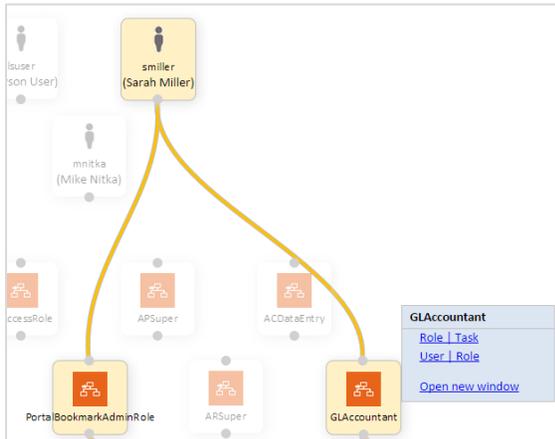
By default the application will display a map of the first 100 users in the system and their corresponding Role/Security Class assignments.



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

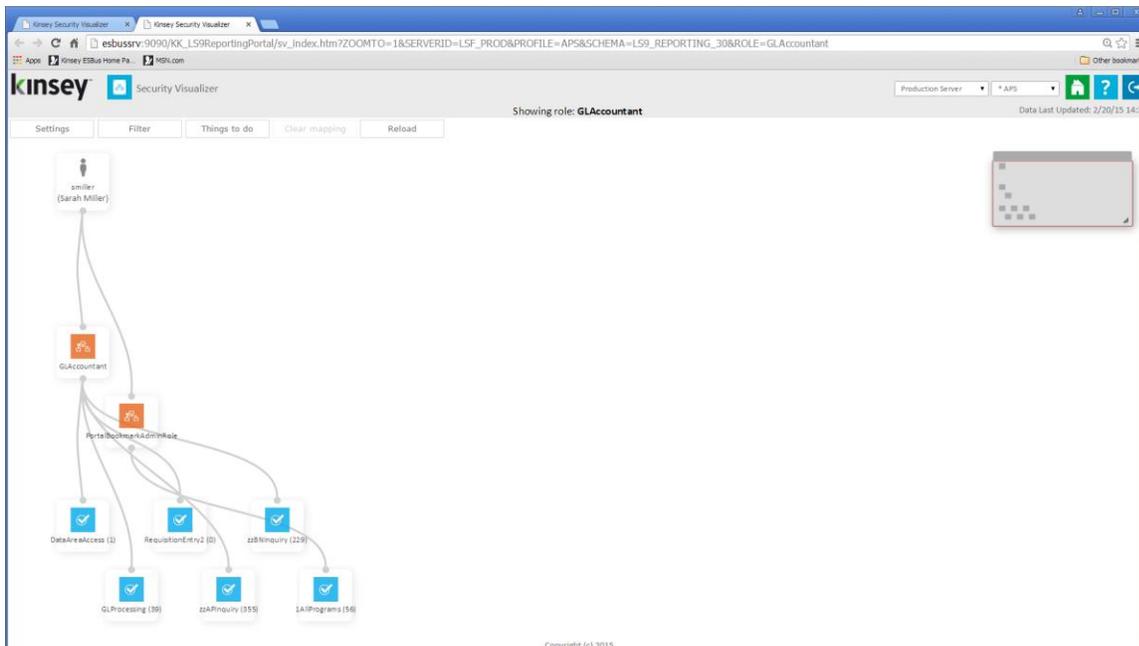
The pop up window allows me to view this mapping in a new window or link to the security LS security reports..



Role	Task	Task Description
GLAccountant	zzAPInquiry	zzAPInquiry
GLAccountant	zzBNInquiry	zzBNInquiry
GLAccountant	DataAreaAccess	DataAreaAccess
GLAccountant	GLProcessing	GL Processing for AP/SL Clerk
GLAccountant	RequestionEntry2	Requestion Entry # 2

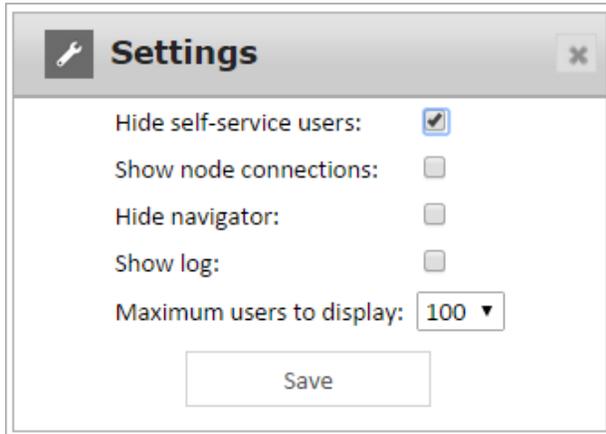
When I selected a report link the appropriate LS report including the filters will be displayed on a new browser page.

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

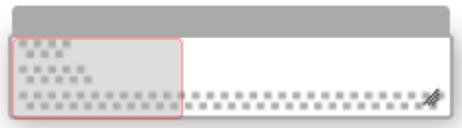
The settings button provides some default options for the current session.



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

Show node connections: The node connections are the lines that link objects when the map is displayed. By defaults the mapping is not displayed until you select a specific 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 the grey shadowed section within the section the map will change orientations.

Show log: This option will display a list of any new or deleted assignments created during the session. The list of changes can then be upload directly 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. There are 3 filters you can use prior to displaying the map:

- Users
- Role
- Security Class

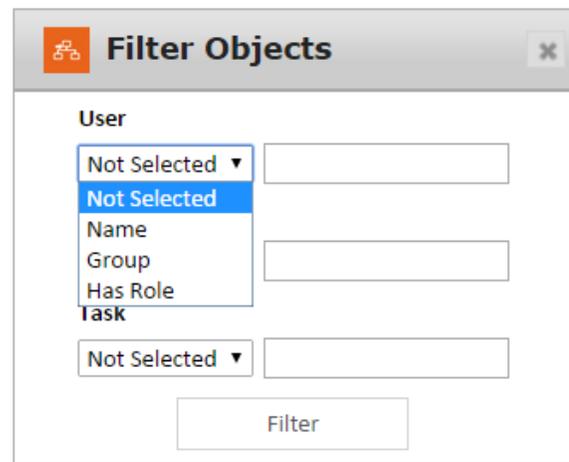
The User filter provides 3 options; user name, group name or all users assigned a specific Role.

The Name option will use the full name of the user assigned in LDAP. This is not the user's 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.

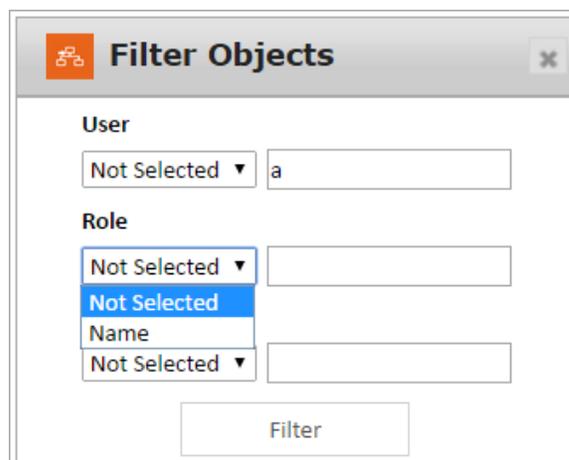
The 'Group' and 'Has Role' filters work the same way utilizing contains logic to build the map.

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 ACEExpert, ARSuper and APSuper will be displayed.



The screenshot shows the 'Filter Objects' dialog box. Under the 'User' section, there are three dropdown menus, each followed by a text input field. The first dropdown is open, showing options: 'Not Selected', 'Name', 'Group', and 'Has Role'. The second dropdown is set to 'Not Selected'. The third dropdown is also set to 'Not Selected'. A 'Filter' button is located at the bottom of the dialog.

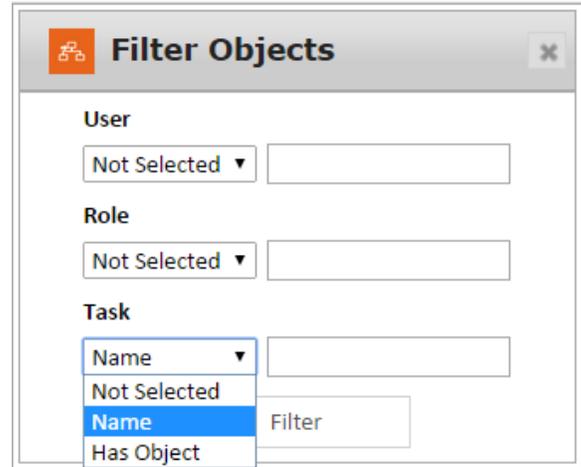


The screenshot shows the 'Filter Objects' dialog box. Under the 'User' section, the first dropdown is set to 'Not Selected' and the text input field contains the letter 'a'. Under the 'Role' section, there are three dropdown menus, each followed by a text input field. The first dropdown is open, showing options: 'Not Selected', 'Name', and 'Not Selected'. The second dropdown is set to 'Not Selected'. The third dropdown is also set to 'Not Selected'. A 'Filter' button is located at the bottom of the dialog.

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

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

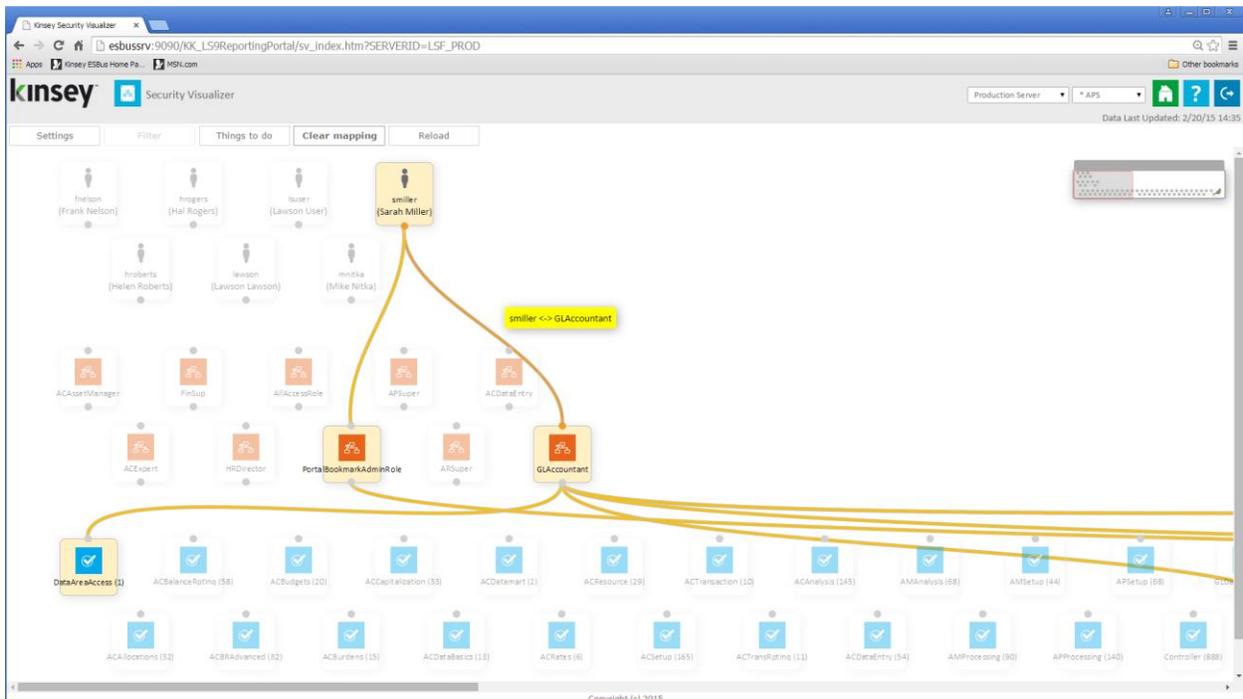
The 'Has Object' option allows you to enter a specific form or table that might be contained in a Security Class. For example if HR11.1 is entered as the Object name all Users, Roles and Security Class linked to HR11.1 will be displayed.



Modifying Role Assignments

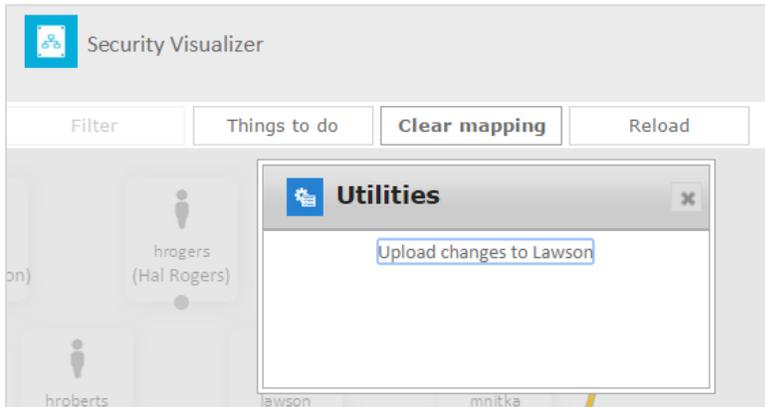
The application will allow you to either add or delete a Role assigned to a specific User.

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



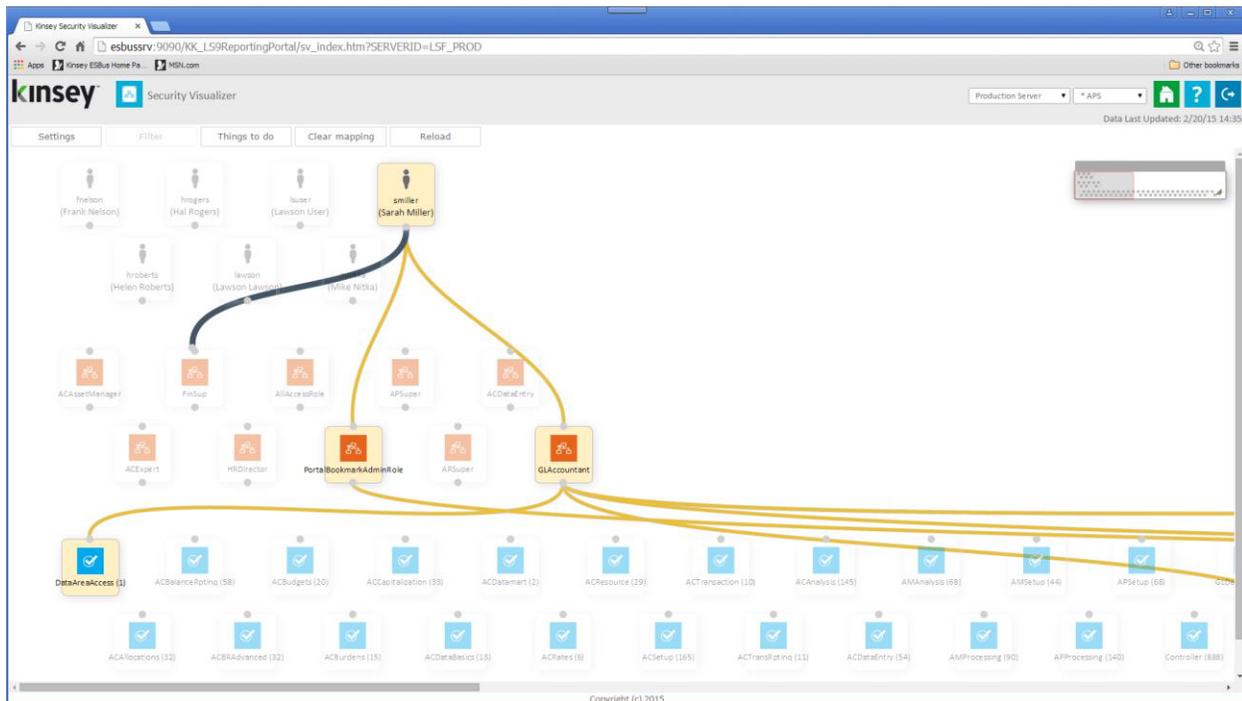
To delete a Role, click on the line that connects the User to the Role. You will received a message box asking you to confirm the delete. If you have 'show log' turned on in settings the action will be displayed in the log window.

To upload the change click on the Things to do button.

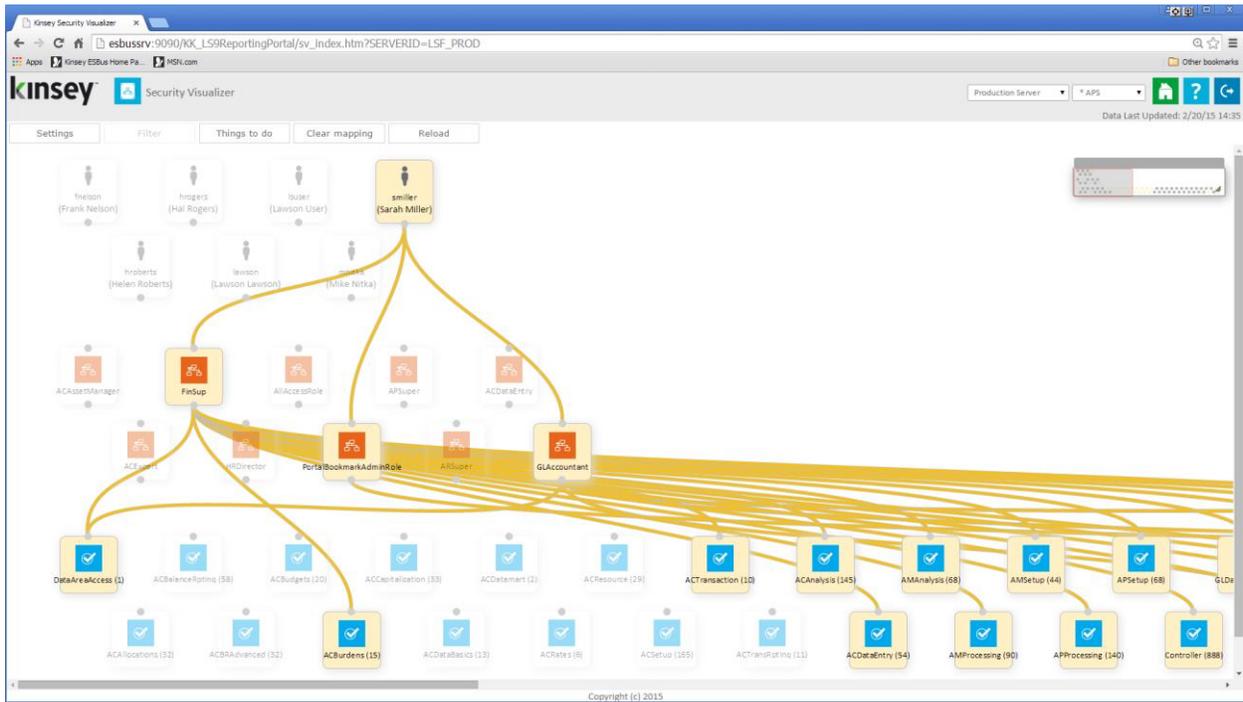


You can upload the change to LDAP provided you have the credentials to log in to the Lawson security administration tool.

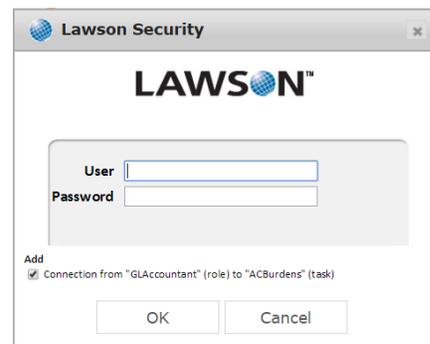
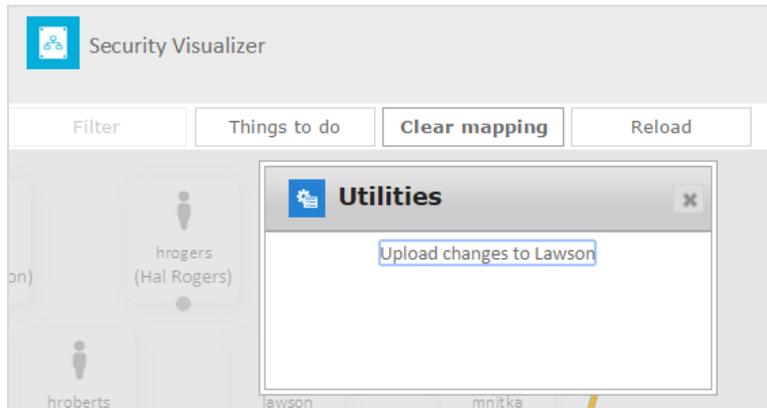
To assign a new Role to a User click on the small circle below the users name and draw a line between that point and the required Role.



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



To upload the change click on the Things to do button.

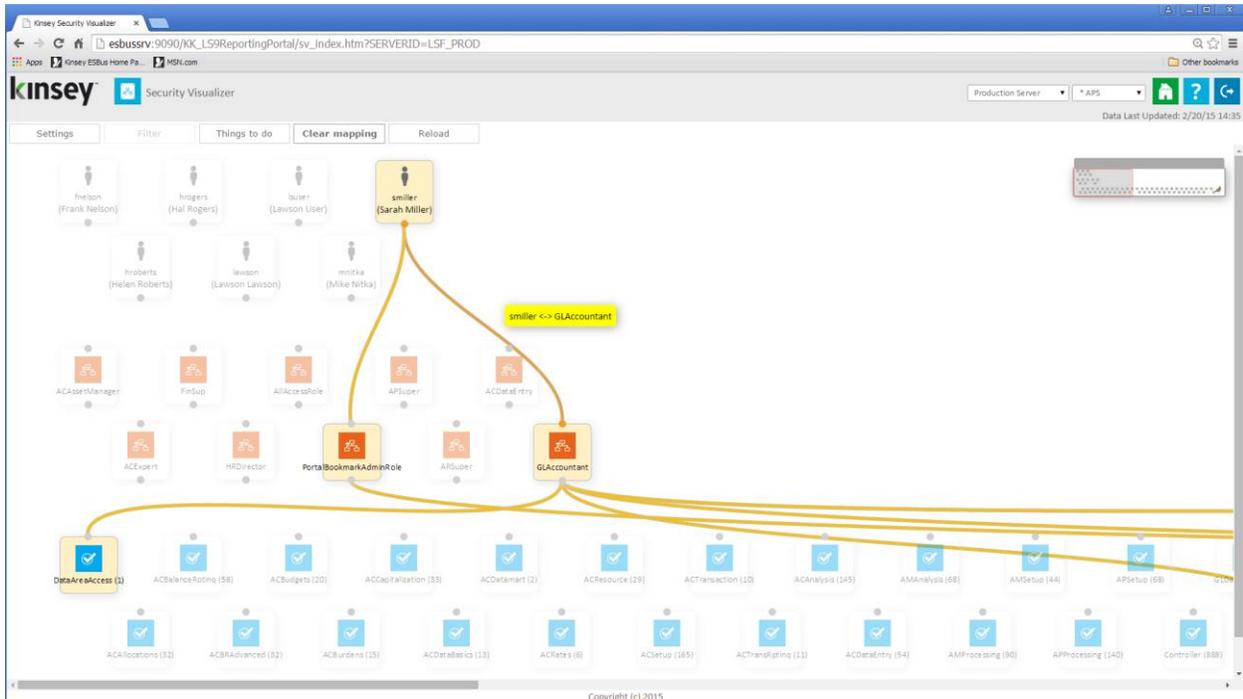


You can then select "Upload changes to Lawson" provided you have the credentials to log in to the Lawson security administration tool.

Modifying Security Class Assignments

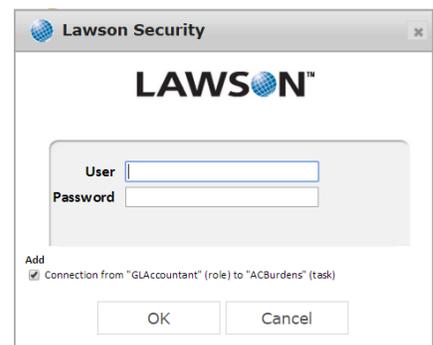
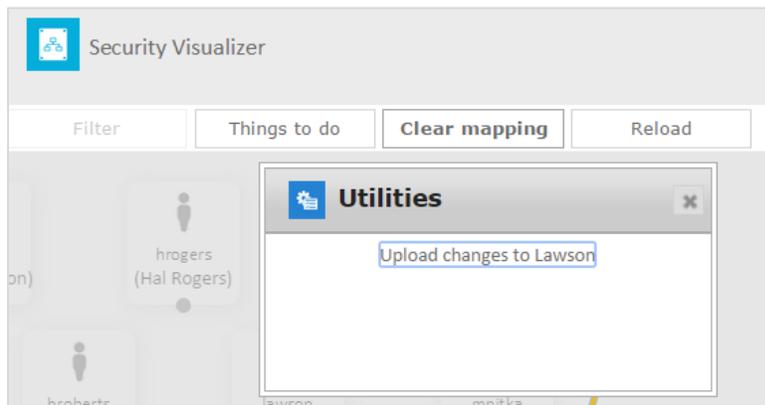
The application will allow you to either add or delete a Security Classes assigned to a specific Role.

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



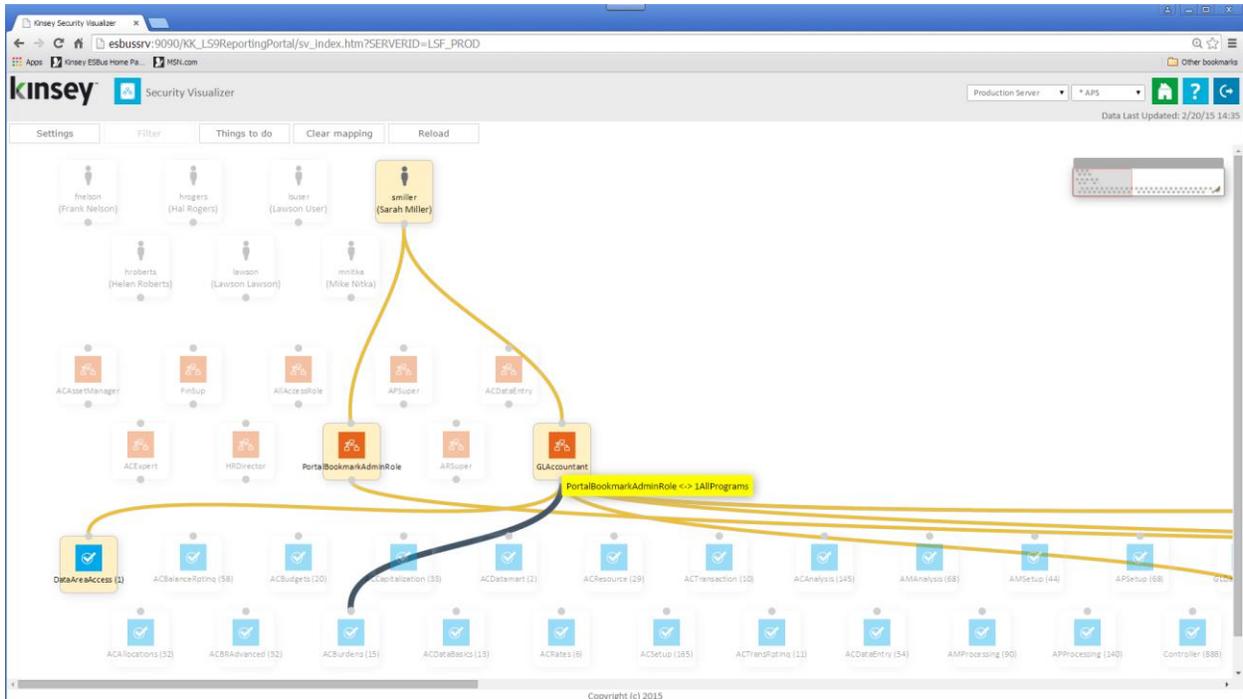
To delete a Security Class, click on the line that connects the Role to the Security Class. You will received a message box asking you to confirm the delete. If you have logging turned on the action will be displayed in the log window.

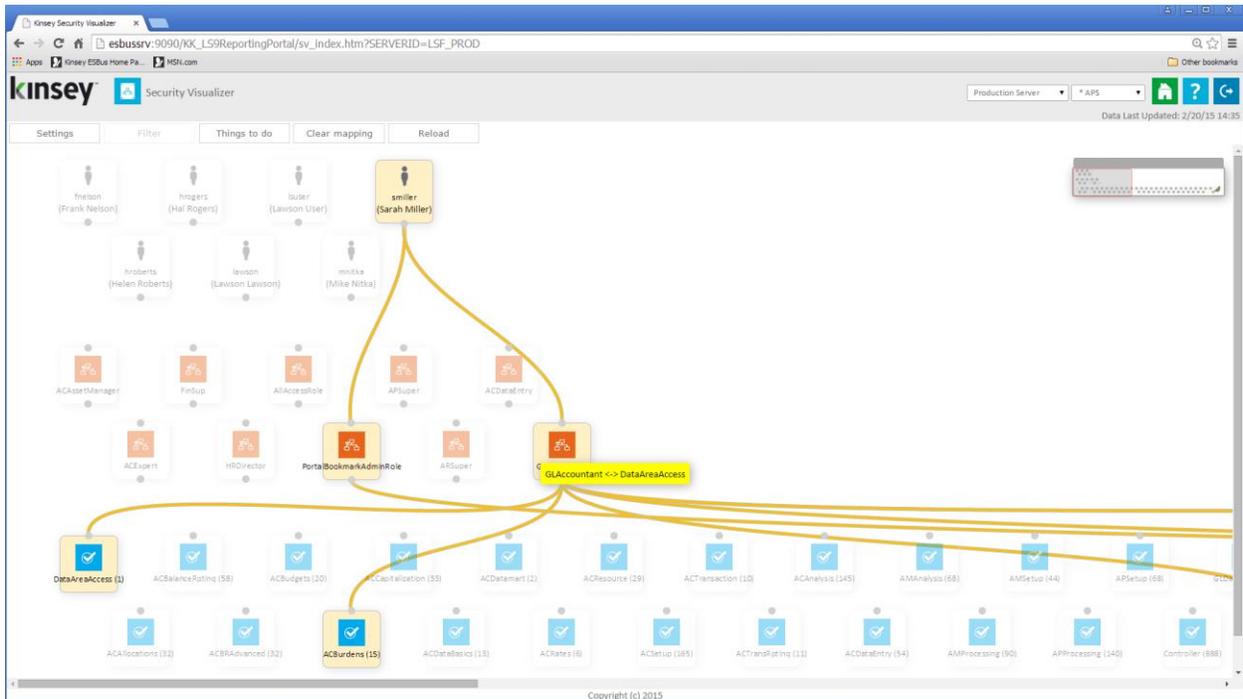
To upload the change click on the Things to do button.



You can then select "Upload changes to Lawson" provided you have the credentials to log in to the Lawson security administration tool.

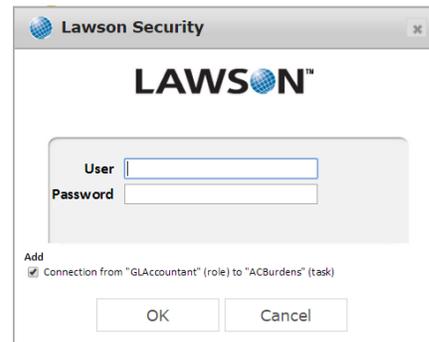
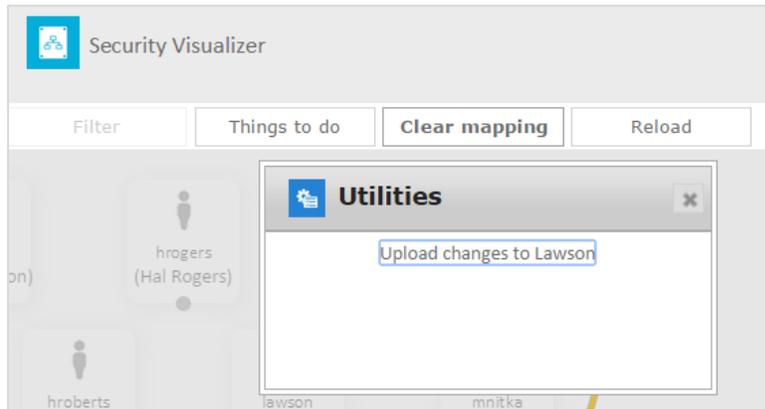
To assign a new Security Class to a Role click on the small circle below the Role name and draw a line between that point and the required Security Class.





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

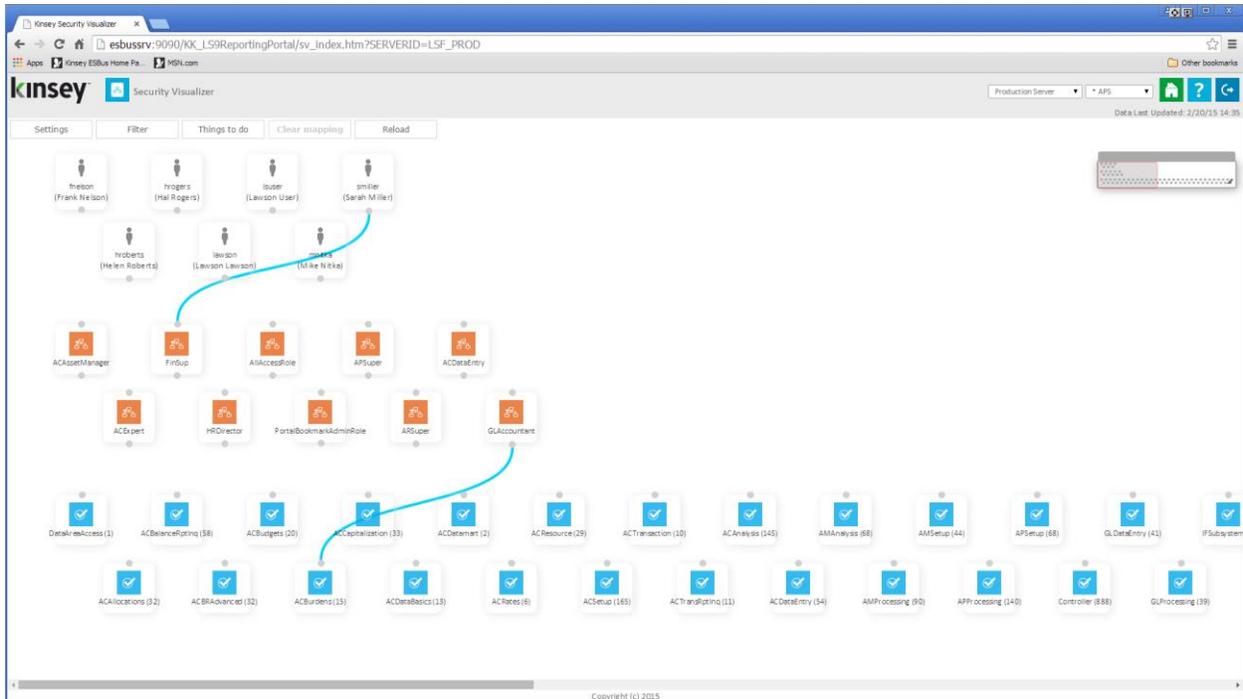
To upload the change click on the Things to do button.



You can then select "Upload changes to Lawson" provided you have the credentials to log in to the Lawson security administration tool.

Clear Mapping

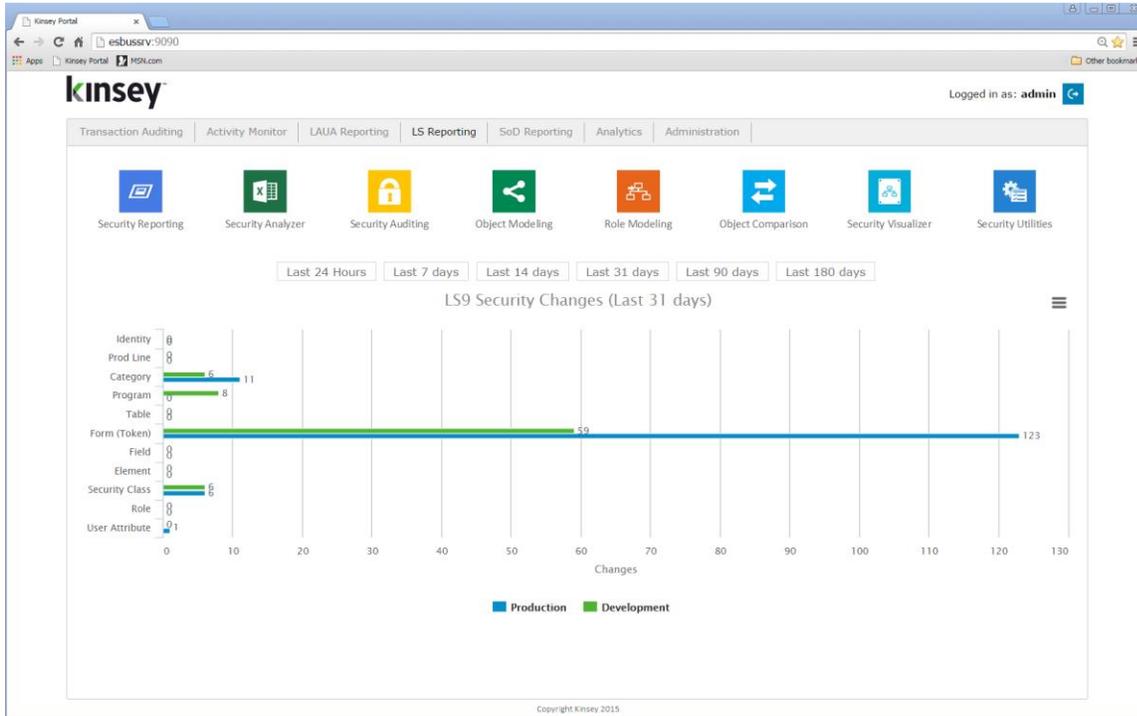
The Clear Mapping button will give you a fresh start on making new assignments. When you clear the map any pending assignments will still be displayed. As you can see in this example the 2 changes made in the prior examples are still shown because they have not been uploaded to Lawson (LDAP).



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

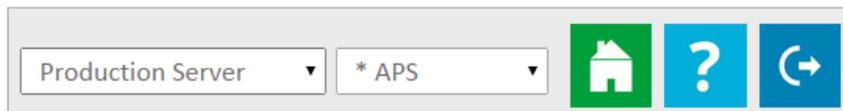
Security Utilities

The Security Utility will allow you to create an inquiry only version of an existing Security Class provided you have the credentials to log into the Lawson Security Admin tool.



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

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



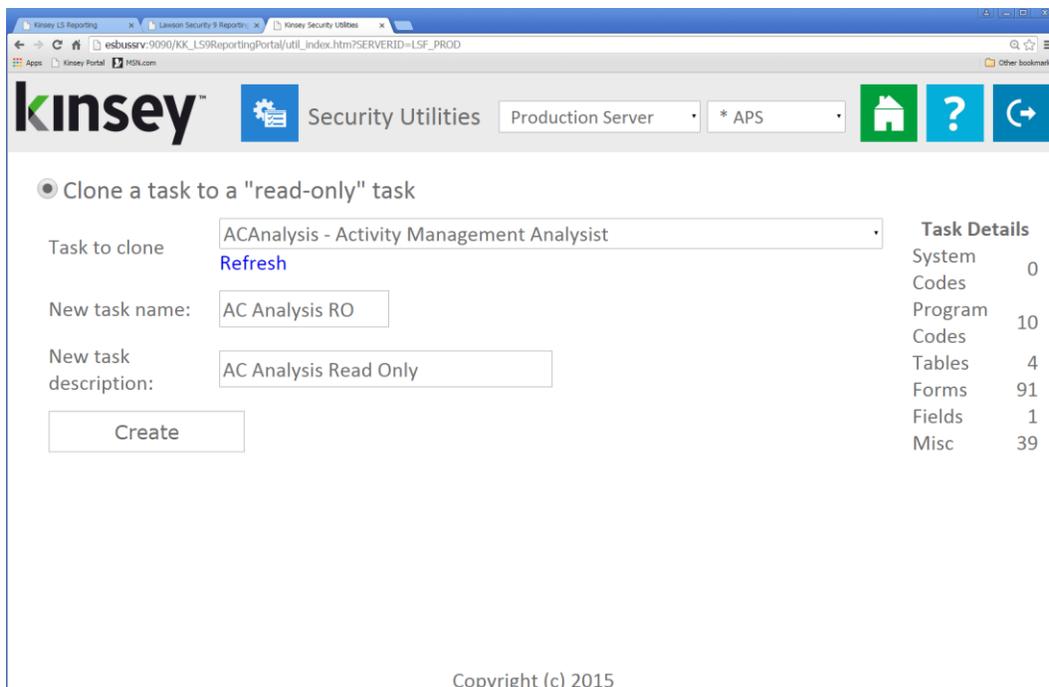
Select the "Clone a Security Class to a 'read-only' Security Class option.

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



A dialog box titled "Lawson Security" with the Lawson logo. It contains two input fields: "User" and "Password". Below the fields are two buttons: "OK" and "Cancel".

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



The Kinsey Security Utilities interface. The main heading is "Clone a task to a 'read-only' task". A dropdown menu is set to "ACAnalysis - Activity Management Analyst", with a "Refresh" link below it. The "New task name:" field contains "AC Analysis RO" and the "New task description:" field contains "AC Analysis Read Only". A "Create" button is at the bottom left. On the right, a "Task Details" table shows the following data:

Task Details	
System Codes	0
Program Codes	10
Tables	4
Forms	91
Fields	1
Misc	39

Copyright (c) 2015

Enter the new Security Class Name and Description and select the Create button.

Trouble Shooting

Why am I missing users and roles from my security reports.

In this case the collection process was either interrupted or the LDAP paging size is not set correctly. You can run the collection process manually by going to the Administration tab, Scheduled Task, LS LDAP collection (PROD or TEST). Once this has completed try running your reports again. If you are still missing information have your system administrator refer to pages 38 and 39 in the Kinsey Administration Guide on how to set the LDAP paging size.

Why don't my S3 security reports reflect my current changes?

The security reports use data store in Kinsey's SQL tables that are updated nightly. Any security changes made during the day will not be reflected on the security report until the following day. To see your changes immediately you can run the scheduled task "**LS LDAP data collection (PROD or TEST)**" manually from the admin panel. For more information on how to run this task refer to the Kinsey Admin Users Guide, Scheduled Task.

Why don't the Security Analyzer report reflect my current changes?

The Security Analyzer uses data store in Kinsey's SQL tables that are updated nightly. Any security changes made during the day will not be reflected on the Security Analyzer report until the following day. To see your changes immediately you can run the scheduled task "**Collect/Update LS Analyzer data (PROD or TEST)**" manually from the admin panel. For more information on how to run this task refer to the Kinsey Admin Users Guide, Scheduled Task.

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

The security audit reports use data store in Kinsey's SQL tables that are updated nightly. Any security changes made during the day will not be reflected on the audit report until the following day. To see your changes immediately you can run the scheduled task "**Collect LS Auditing data (using ERP HTTP Call) (PROD or TEST)**" manually from the admin panel. For more information on how to run this task refer to the Kinsey Admin Users Guide, Scheduled Task.

Why don't I have any security snapshots to select from when generating security reportings.

Security snapshots are create in the Administration panel under Scheduled Tasks. Your administrator of the Kinsey dashboard will need to run the task "Snapshot - LS LDAP" for either TEST or PROD.

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

The security reports use data store in Kinsey's SQL tables that are updated nightly. Any security changes made during the day will not be reflected on the security report until the following day. To see your changes immediately you can run the scheduled task **"Landmark data collection (PROD or TEST)"** manually from the admin panel. For more information on how to run this task refer to the Kinsey Admin Users Guide, Scheduled Task.

Notes: