kinsey™

Segregation of Duties
User Guide

Document contains instructions related to Segregation of Duties reporting

2019

Contents

Introduction

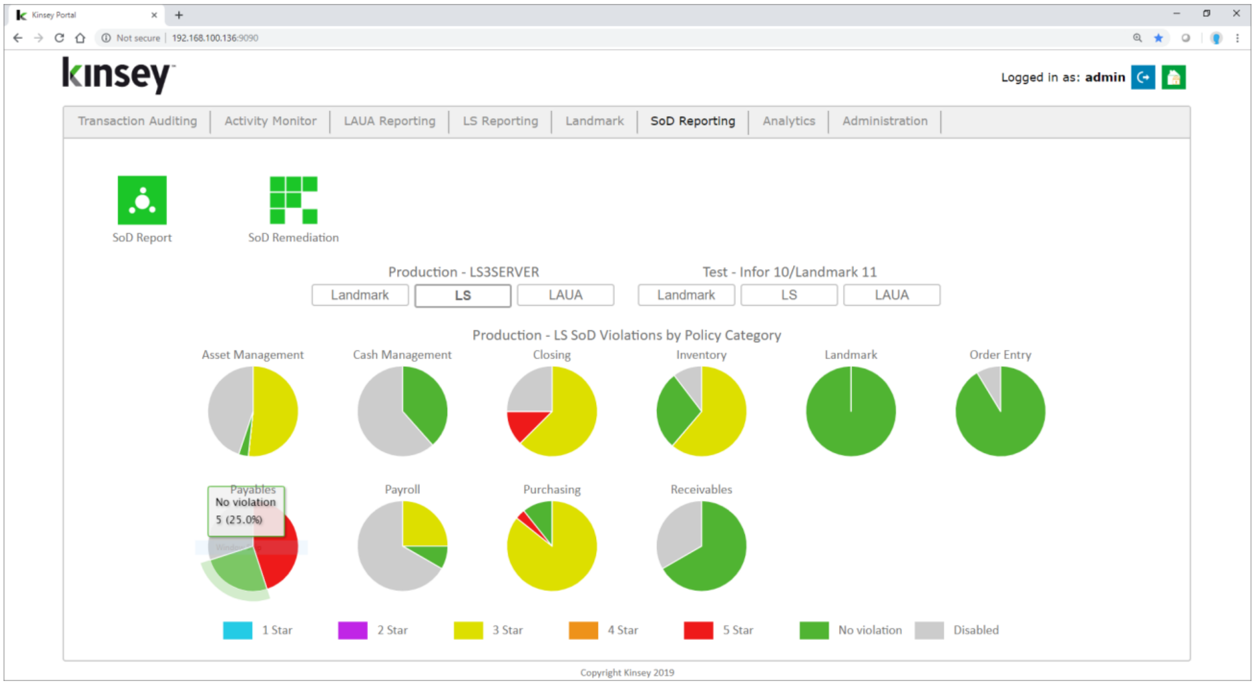
Kinsey’s Segregation of Duties (SoD) Reporting is designed to examine Lawson S3, LAUA and Landmark Security to determine if the proper checks and balances are being following in the respective security models. The delivered policies cover applications included in all 3 Lawson product suites. The policies delivered have been accumulated over a number of years based on research and customer recommendations. The rules applied to these policies are Kinsey’s best interpretation of the policy but should be verified by the customer during the implementation phase. An unlimited number of new policies can be added or existing policies can be modified to align with your organization. The SoD report can be generated at any time by an authorized user and will identify the policies that have been violated and the specific assignments that have caused the violation.

Features:

- Delivered with over 280 Segregation of Duties policies
- Ability to add an unlimited number of policies and rules
- Ability to activate and rank policies individually
- Predefined reports by User, by Policy or by User Role grouping
- Excel export options
- Differences Reporting

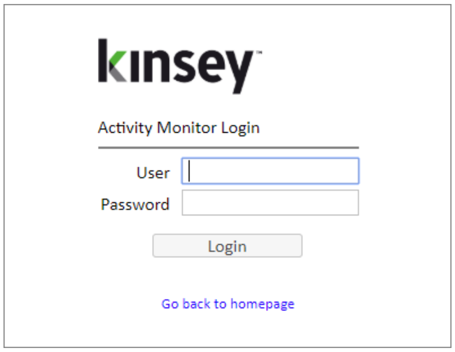
Getting Started

Your system administrator will provide the URL to access the Kinsey security dashboard. Select the SoD Reporting tab to access the application. The page displays the current number of policy violations based on the policy rating.

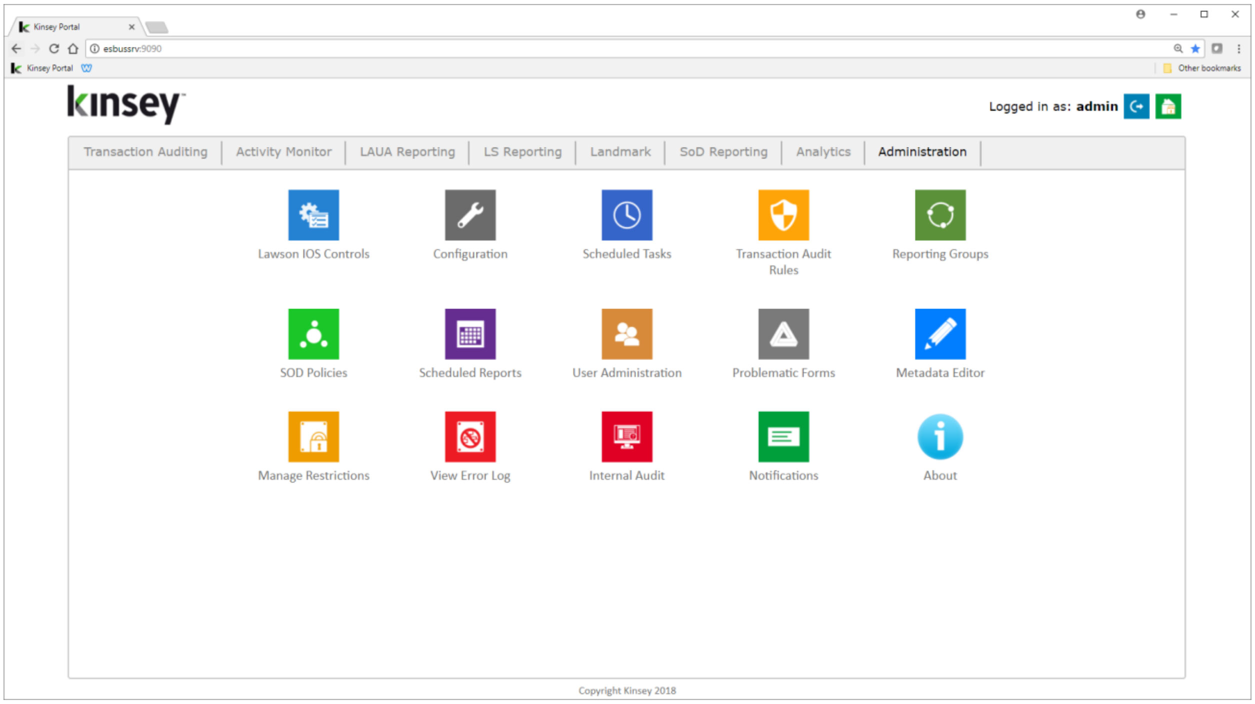


Logging in

If you have not previously logged into the application you will be required to enter your credentials. If you have not been provided login credential see your system administrator.



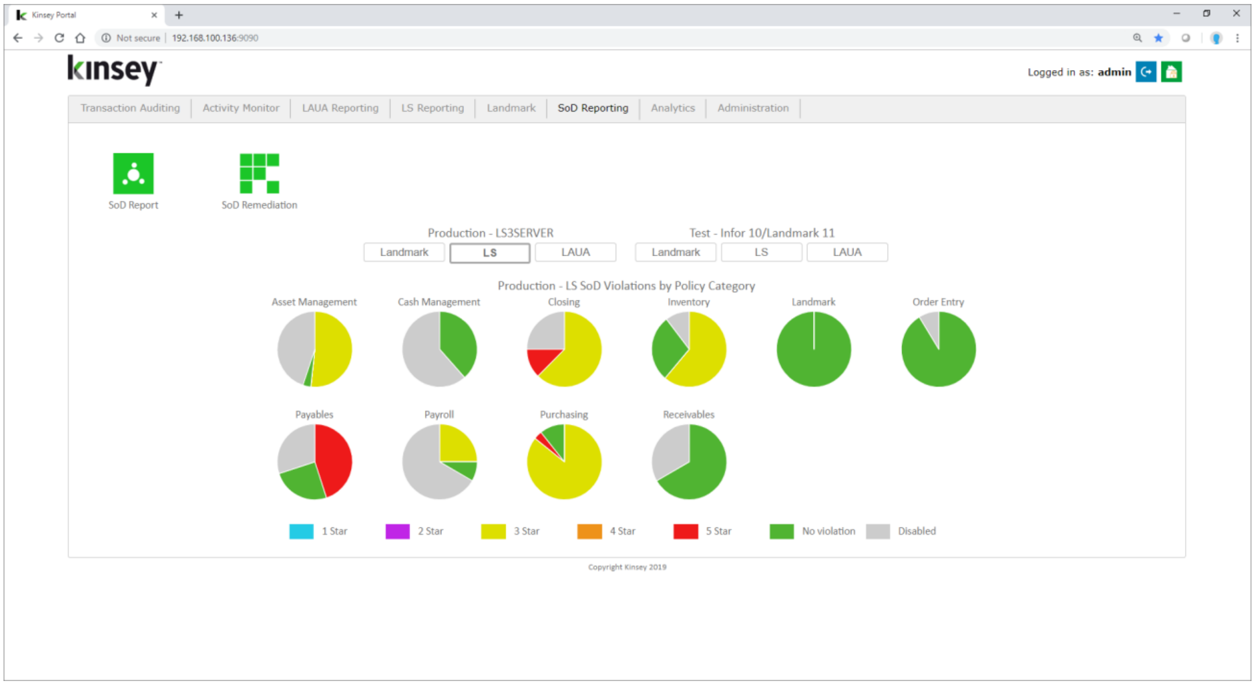
Administration



Policy Maintenance

Refer to the SoD policy Maintenance section of the Kinsey Administrator Guide for information on how to create and maintain SoD policies.

Reporting

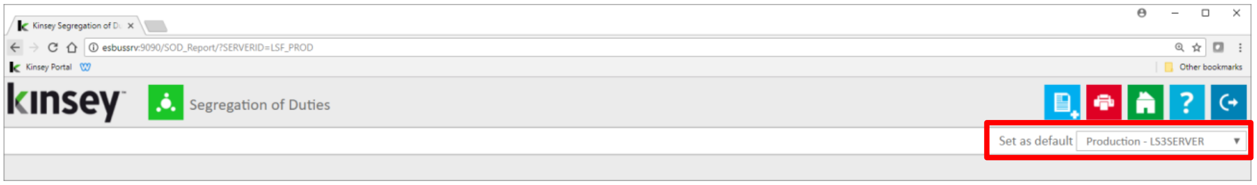


The dashboard will display a pie chart for up to 12 policy categories. By default the application display's charts for the LS Production environment with additional options for both the LAUA and Landmark Production and Test environments.

There are potentially 7 colors that could be displayed on each chart.

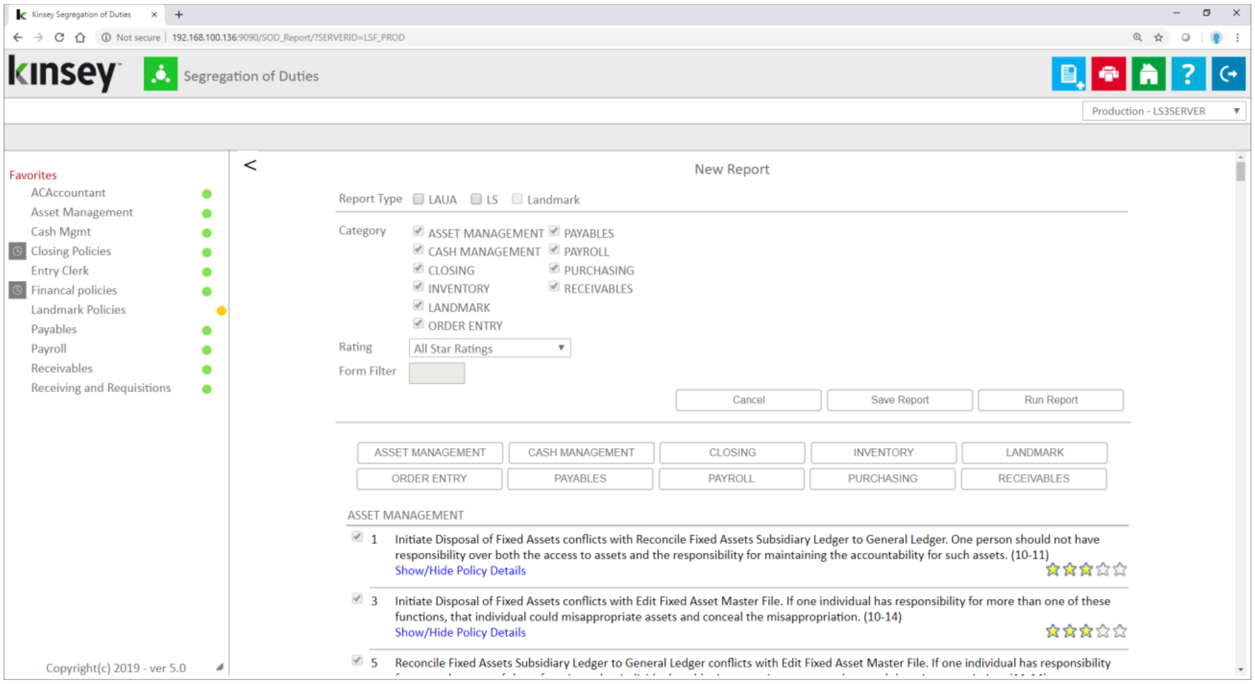
○	Green	No Violations
○	Grey	Disabled Policies
○	Red	5 Star policies in violation
○	Orange	4 Star policies in violation
○	Yellow	3 Star policies in violation
○	Purple	2 Star policies in violation
○	Navy Blue	1 Star policies in violation

When you first enter the SoD reporting page you will need to select the appropriate server that contains your Lawson application. Use the drop down box to select the server.



Creating a New Report

To define a new report click on the Add Report icon on the title bar



New Report

Report Type ☐ LAUA ☐ LS ☐ Landmark

Category ☑ ASSET MANAGEMENT ☑ PAYABLES ☑ CASH MANAGEMENT ☑ PAYROLL ☑ CLOSING ☑ PURCHASING ☑ INVENTORY ☑ RECEIVABLES ☑ LANDMARK ☑ ORDER ENTRY

Rating: All Star Ratings

Form Filter:

ASSET MANAGEMENT

☑ 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 ★★★☆☆

☑ 5 Reconcile Fixed Assets Subsidiary Ledger to General Ledger conflicts with Edit Fixed Asset Master File. If one individual has responsibility

The page will display a list of options you can use to filter the policies you want included on your report. Begin by selecting the LAUA, LS or Landmark check box for the security model you would like to validate.

There are two types of reports you can define when creating a new report.

- Security Class Violation Report – this report will show all violations for each LS User, each Landmark User or for each LAUA Security Class depending on the security model selected.
- Role Test Report – this report will report on violations for any Role or Role combinations in LS or Landmark security. This is not an option for LAUA security.

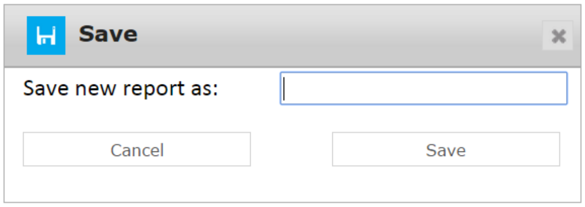
To create a new SoD violation report use the Category, Level of Importance (star rating) and Form filters to make your selections.

Category: By default all categories are selected when you define a new report. Simply uncheck a category to omit those policies from the report.

Level of Importance: The policy list can be restricted based with the star rating assigned to each policy. See “Rating a Policy’s Level of Importance” in the Kinsey Administration Guide for more information.

Form Filter: The form filter will display all policies that include the form entered in this field or you can expand the list by entering only a portion of the form name. For example, if you want all policies that contain AP10.1 enter AP10.1 in the Form Filter field. However, if you want all forms that include AP tokens just enter AP into the field. The system uses the entry as a 'contains in' filter.

Once you have made your selection you can either run the report or save report for future use. To run the report simply select the Run Report button on the screen. To save the report select Save Report and enter a report name.

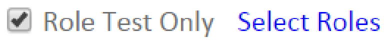


Note: the system does not store the Form filter or the Level of Importance with the report parameters, rather it stores the actual policies selected. If you edit an existing report you can revise your policy list by using the check box next to the policy number. See Editing a Report for more information

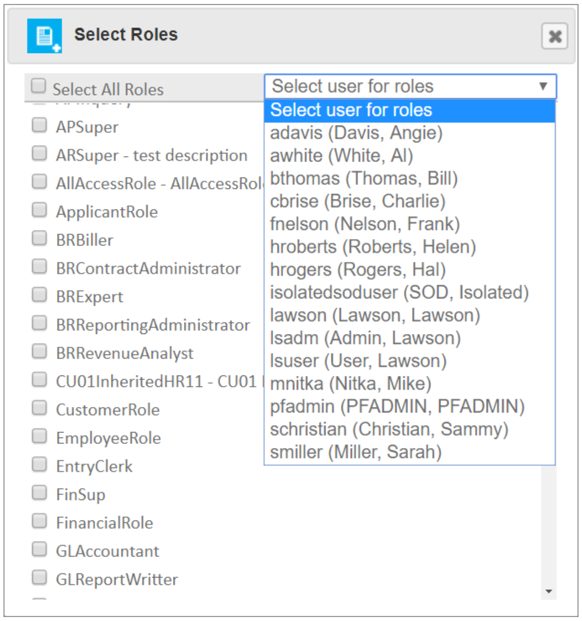
Creating a Role Test Report (Lawson and Landmark Security only)

The Role Test report incorporates a "Role selection" filter to the filter parameters described in the New Report section of this manual. The Role filter allows you to test a list of policies against a specific role or combination of roles.

Start by making the same selections you would for a User violation report then check the *Role Test Only* check box and select the roles link to view a list of the roles you have defined.



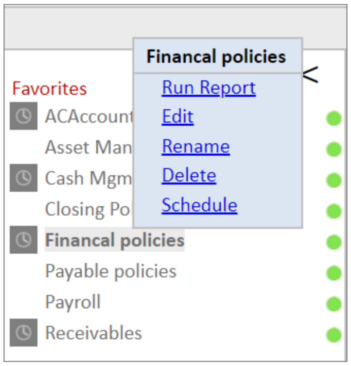
When the list of roles is displayed you can choose any combination of roles or select an existing user from the dropdown window. When you select a user the roles assigned to them will automatically be checked. You can then check any other role you might want to add to this user. When you are finished making your selection close the window to continue.



You can now either run the report or save report for future use. To run the report simply select the Run Report button on the screen. To save the report select Save Report, enter a report name and Save.

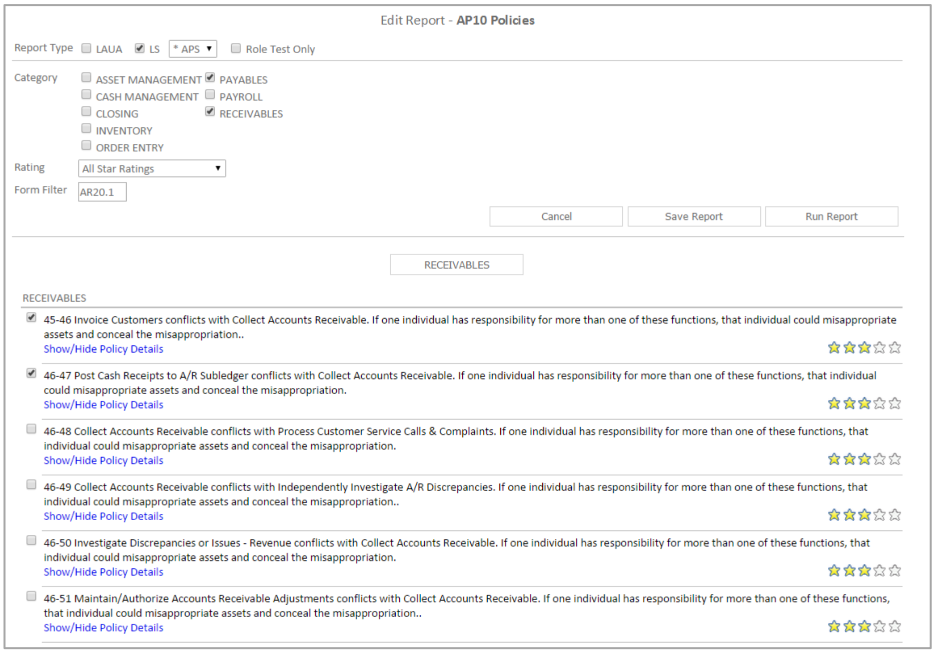
Editing an Existing Report

To edit an existing report click on the report name under Favorites and select Edit.



The edit option will display the same set of parameters as found when creating a new report. When a new report is saved the categories selected and the list of policies are saved based on the filter criteria. The original level of importance (star rating) and the form filter selections do not need to be saved because the actual policies are instead.

You can remove policies from the report by using the check box next to the policy. To add policies not displayed on the screen select another set of filter criteria.



Edit Report - **AP10 Policies**

Report Type □ LAUA ☑ LS * APS ▾ □ Role Test Only

Category □ ASSET MANAGEMENT ☑ PAYABLES
□ CASH MANAGEMENT □ PAYROLL
□ CLOSING ☑ RECEIVABLES
□ INVENTORY
□ ORDER ENTRY

Rating All Star Ratings ▾

Form Filter AR20.1

RECEIVABLES

☑ 45-46 Invoice Customers conflicts with Collect Accounts Receivable. If one individual has responsibility for more than one of these functions, that individual could misappropriate assets and conceal the misappropriation..
Show/Hide Policy Details ★★★☆☆

☑ 46-47 Post Cash Receipts to A/R Subledger conflicts with Collect Accounts Receivable. If one individual has responsibility for more than one of these functions, that individual could misappropriate assets and conceal the misappropriation.
Show/Hide Policy Details ★★★☆☆

□ 46-48 Collect Accounts Receivable conflicts with Process Customer Service Calls & Complaints. If one individual has responsibility for more than one of these functions, that individual could misappropriate assets and conceal the misappropriation.
Show/Hide Policy Details ★★★☆☆

□ 46-49 Collect Accounts Receivable conflicts with Independently Investigate A/R Discrepancies. If one individual has responsibility for more than one of these functions, that individual could misappropriate assets and conceal the misappropriation..
Show/Hide Policy Details ★★★☆☆

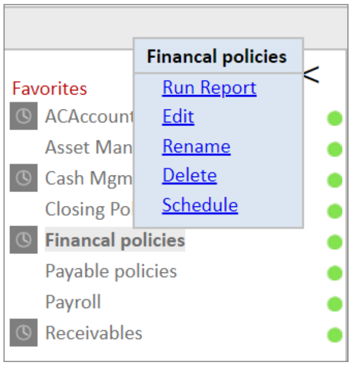
□ 46-50 Investigate Discrepancies or Issues - Revenue conflicts with Collect Accounts Receivable. If one individual has responsibility for more than one of these functions, that individual could misappropriate assets and conceal the misappropriation.
Show/Hide Policy Details ★★★☆☆

□ 46-51 Maintain/Authorize Accounts Receivable Adjustments conflicts with Collect Accounts Receivable. If one individual has responsibility for more than one of these functions, that individual could misappropriate assets and conceal the misappropriation..
Show/Hide Policy Details ★★★☆☆

Note: The key to editing a report is to ensure that the policies you want included on the report are displayed on the screen before you save the report.

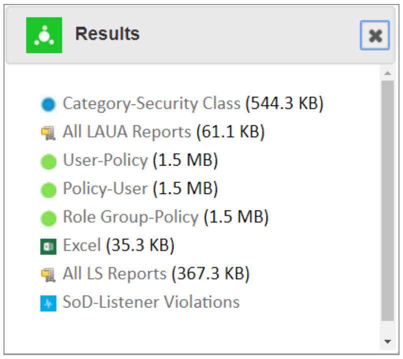
Running a Saved Report

To run a saved report simply click on the report name and select Run Report. You can immediately view the report in your browser or save the file to be viewed at a later time.



The color of the dot next to the report indicates the security model being checked. A blue dot indicates LAUA, green is for LS and orange is used for Landmark.

When the report is finished the report options will be displayed in the top left corner of the navigation pane.


Results
Category-Security Class (544.3 KB)
All LAUA Reports (61.1 KB)
User-Policy (1.5 MB)
Policy-User (1.5 MB)
Role Group-Policy (1.5 MB)
Excel (35.3 KB)
All LS Reports (367.3 KB)
SoD-Listener Violations

The zipped report contains the HTML reports and the MS Excel document. This file can be distributed to anyone unable to run reports that may need to analyze the results.

Category – Security Class (LAUA only)

The LAUA Report provides a list of violations sorted by Category and Policy showing the Security Classes in violation. (See page 14)

User-Policy (LS and Landmark)

This report provides a list of User's and the policies they are currently violating. (See page 15)

Policy User (LS and Landmark)

This report provides a list of Policies and the User's in violation. Policy are grouped by SoD Category. (See page 15)

Role Group-Policy (LS and Landmark)

This report dynamically groups all users together based on their assigned security roles. Users with the exact same Role assignment are put together in a group for this report. By doing this you can evaluate a group of users sharing the same Role assigment that are violating any particular policy. (See page 16)

Differences Report

The differences report will show you any report changes since the last time the report was run. The report is sorted by User the Policy.

Renaming a Report

To rename an existing report click on the report name and select Rename.

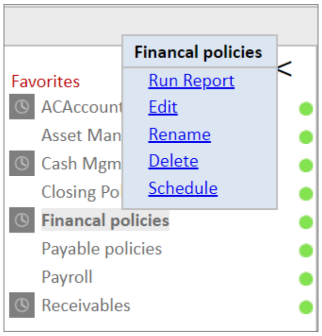
Deleting a Report

To rename an existing report click on the report name and select *Delete*.

Scheduling a Report

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

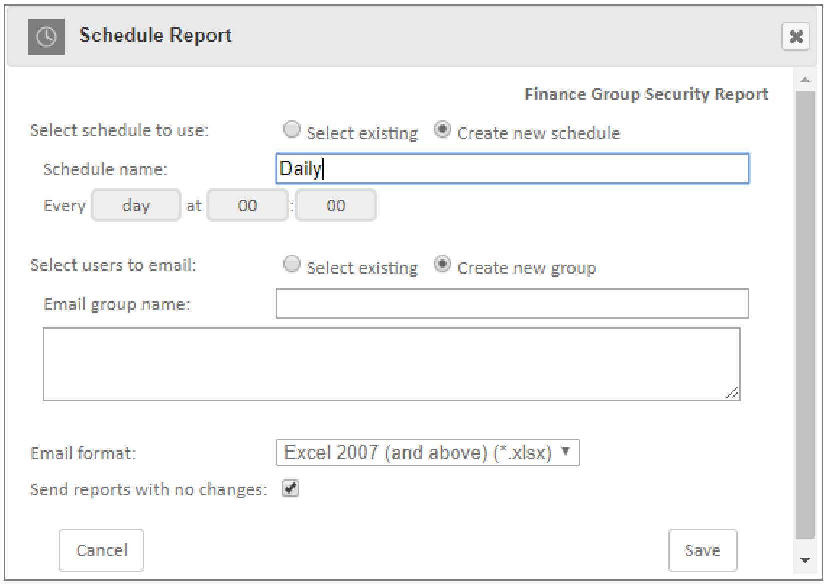
To schedule a report you must first create and save your report. Once the report displays under saved reports in the left navigation pane, click on the report name and select Schedule.



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 active (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: Daily

Every day at 00 : 00

Select users to email: ○ Select existing ● Create new group

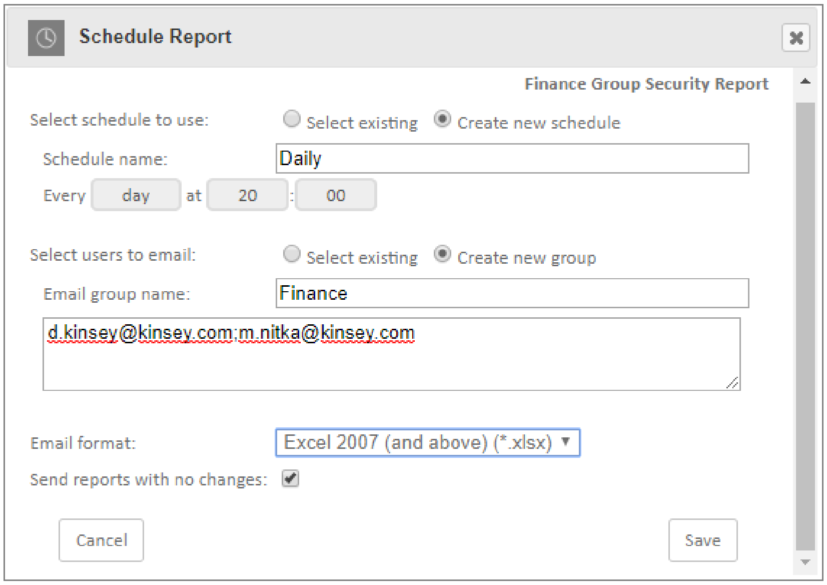
Email group name:

Email format: Excel 2007 (and above) (*.xlsx)

Send reports with no changes: ☑

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.



Schedule Report

Finance Group Security Report

Select schedule to use: ○ Select existing ● Create new schedule

Schedule name: Daily

Every day at 20 : 00

Select users to email: ○ Select existing ● Create new group

Email group name: Finance

d.kinsey@kinsey.com;m.nitka@kinsey.com

Email format: Excel 2007 (and above) (*.xlsx)

Send reports with no changes: ☑

Email format:

The export options are Excel or Adobe PDF

Send blank reports:

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

Note: any Schedule or Email Group created at this time can also be used with other Kinsey applications.

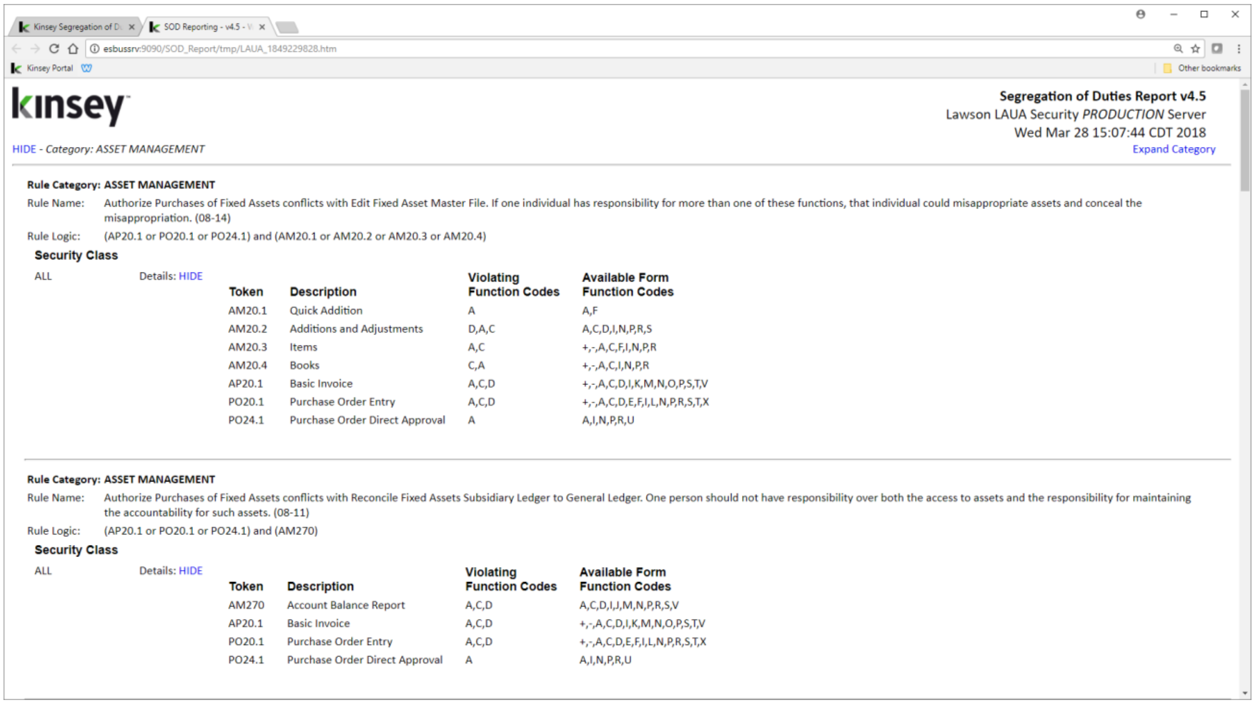
Activating or Deactivating a Scheduled Report

To change the activation status of a schedule you need to access the Schedule Reports option on the Administration tab. Refer to Scheduled Reports in the Kinsey Admin Guide for details on how to manage scheduled reports.

Report Formats

To print any of the selected reports select the red printer icon on the title bar.

By Security Class (LAUA)



Segregation of Duties Report v4.5
Lawson LAUA Security *PRODUCTION* Server
Wed Mar 28 15:07:44 CDT 2018

HIDE - *Category: ASSET MANAGEMENT*

Expand Category

Rule Category: ASSET MANAGEMENT

Rule Name: Authorize Purchases 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. (08-14)

Rule Logic: (AP20.1 or PO20.1 or PO24.1) and (AM20.1 or AM20.2 or AM20.3 or AM20.4)

Security Class

ALL Details: HIDE

Token	Description	Violating Function Codes	Available Form Function Codes
AM20.1	Quick Addition	A	A,F
AM20.2	Additions and Adjustments	D,A,C	A,C,D,I,N,P,R,S
AM20.3	Items	A,C	+,-,A,C,F,I,N,P,R
AM20.4	Books	C,A	+,-,A,C,I,N,P,R
AP20.1	Basic Invoice	A,C,D	+,-,A,C,D,I,K,M,N,O,P,S,T,V
PO20.1	Purchase Order Entry	A,C,D	+,-,A,C,D,E,F,I,L,N,P,R,S,T,X
PO24.1	Purchase Order Direct Approval	A	A,I,N,P,R,U

Rule Category: ASSET MANAGEMENT

Rule Name: Authorize Purchases 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. (08-11)

Rule Logic: (AP20.1 or PO20.1 or PO24.1) and (AM270)

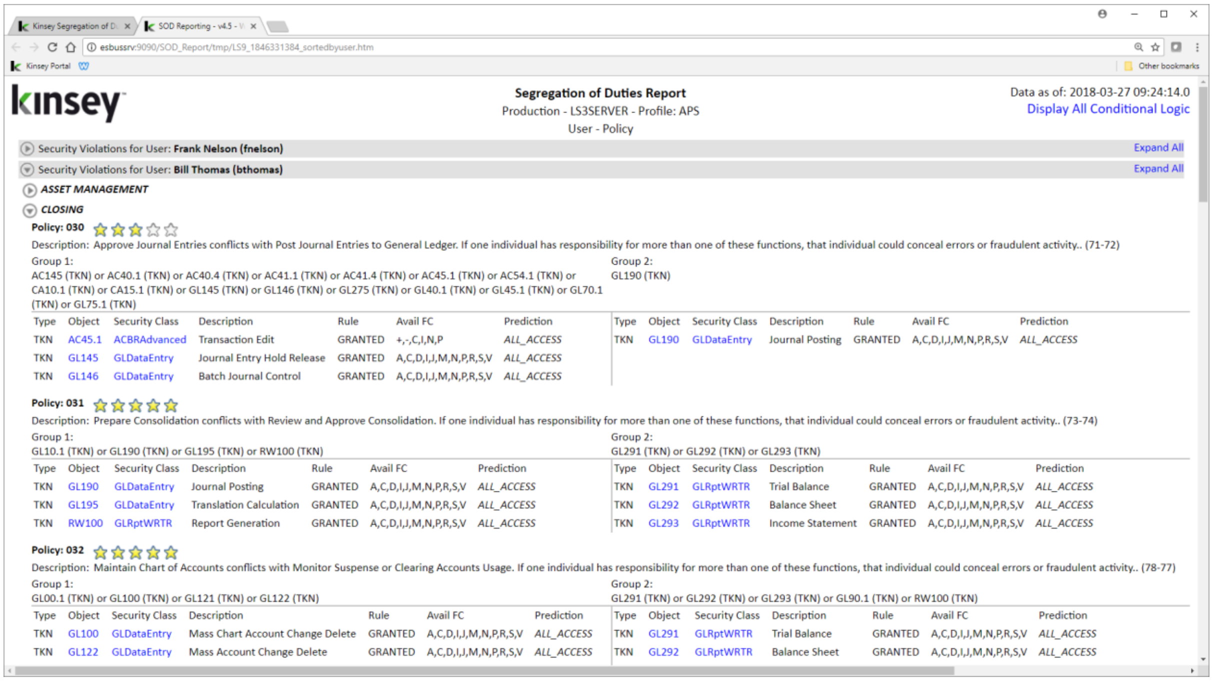
Security Class

ALL Details: HIDE

Token	Description	Violating Function Codes	Available Form Function Codes
AM270	Account Balance Report	A,C,D	A,C,D,I,J,M,N,P,R,S,V
AP20.1	Basic Invoice	A,C,D	+,-,A,C,D,I,K,M,N,O,P,S,T,V
PO20.1	Purchase Order Entry	A,C,D	+,-,A,C,D,E,F,I,L,N,P,R,S,T,X
PO24.1	Purchase Order Direct Approval	A	A,I,N,P,R,U

The Security Class report shows all violations for each LAUA Security Class.

User- Policy Violation Report (LS and Landmark)



Segregation of Duties Report
Production - LS3SERVER - Profile: APS
User - Policy

Data as of: 2018-03-27 09:24:14.0
Display All Conditional Logic

Security Violations for User: **Frank Nelson (fnelson)** Expand All

Security Violations for User: **Bill Thomas (bthomas)** Expand All

ASSET MANAGEMENT

CLOSING

Policy: 030 ★★★☆☆

Description: Approve Journal Entries conflicts with Post Journal Entries to General Ledger. If one individual has responsibility for more than one of these functions, that individual could conceal errors or fraudulent activity.. (71-72)

Group 1:
AC145 (TKN) or AC40.1 (TKN) or AC40.4 (TKN) or AC41.1 (TKN) or AC41.4 (TKN) or AC45.1 (TKN) or AC54.1 (TKN) or CA10.1 (TKN) or CA15.1 (TKN) or GL145 (TKN) or GL146 (TKN) or GL275 (TKN) or GL40.1 (TKN) or GL45.1 (TKN) or GL70.1 (TKN) or GL75.1 (TKN)

Type	Object	Security Class	Description	Rule	Avail FC	Prediction
TKN	AC45.1	ACBRAdvanced	Transaction Edit	GRANTED	+,-,C,I,N,P	*ALL_ACCESS*
TKN	GL145	GLDataEntry	Journal Entry Hold Release	GRANTED	A,C,D,I,J,M,N,P,R,S,V	*ALL_ACCESS*
TKN	GL146	GLDataEntry	Batch Journal Control	GRANTED	A,C,D,I,J,M,N,P,R,S,V	*ALL_ACCESS*

Group 2:
GL190 (TKN)

Type	Object	Security Class	Description	Rule	Avail FC	Prediction
TKN	GL190	GLDataEntry	Journal Posting	GRANTED	A,C,D,I,J,M,N,P,R,S,V	*ALL_ACCESS*

Policy: 031 ★★★★★

Description: Prepare Consolidation conflicts with Review and Approve Consolidation. If one individual has responsibility for more than one of these functions, that individual could conceal errors or fraudulent activity.. (73-74)

Group 1:
GL10.1 (TKN) or GL190 (TKN) or GL195 (TKN) or RW100 (TKN)

Type	Object	Security Class	Description	Rule	Avail FC	Prediction
TKN	GL190	GLDataEntry	Journal Posting	GRANTED	A,C,D,I,J,M,N,P,R,S,V	*ALL_ACCESS*
TKN	GL195	GLDataEntry	Translation Calculation	GRANTED	A,C,D,I,J,M,N,P,R,S,V	*ALL_ACCESS*
TKN	RW100	GLRptWRTR	Report Generation	GRANTED	A,C,D,I,J,M,N,P,R,S,V	*ALL_ACCESS*

Group 2:
GL291 (TKN) or GL292 (TKN) or GL293 (TKN)

Type	Object	Security Class	Description	Rule	Avail FC	Prediction
TKN	GL291	GLRptWRTR	Trial Balance	GRANTED	A,C,D,I,J,M,N,P,R,S,V	*ALL_ACCESS*
TKN	GL292	GLRptWRTR	Balance Sheet	GRANTED	A,C,D,I,J,M,N,P,R,S,V	*ALL_ACCESS*
TKN	GL293	GLRptWRTR	Income Statement	GRANTED	A,C,D,I,J,M,N,P,R,S,V	*ALL_ACCESS*

Policy: 032 ★★★★★

Description: Maintain Chart of Accounts conflicts with Monitor Suspense or Clearing Accounts Usage. If one individual has responsibility for more than one of these functions, that individual could conceal errors or fraudulent activity.. (78-77)

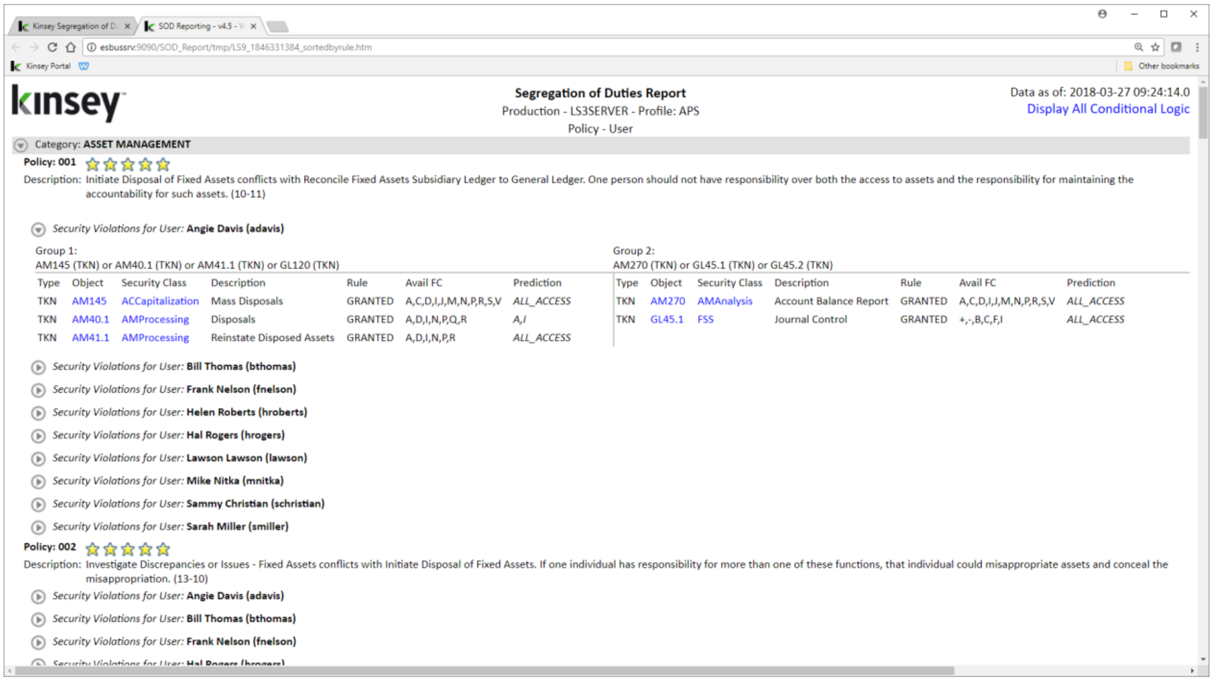
Group 1:
GL00.1 (TKN) or GL100 (TKN) or GL121 (TKN) or GL122 (TKN)

Type	Object	Security Class	Description	Rule	Avail FC	Prediction
TKN	GL100	GLDataEntry	Mass Chart Account Change Delete	GRANTED	A,C,D,I,J,M,N,P,R,S,V	*ALL_ACCESS*
TKN	GL122	GLDataEntry	Mass Account Change Delete	GRANTED	A,C,D,I,J,M,N,P,R,S,V	*ALL_ACCESS*

Group 2:
GL291 (TKN) or GL292 (TKN) or GL293 (TKN) or GL90.1 (TKN) or RW100 (TKN)

Type	Object	Security Class	Description	Rule	Avail FC	Prediction
TKN	GL291	GLRptWRTR	Trial Balance	GRANTED	A,C,D,I,J,M,N,P,R,S,V	*ALL_ACCESS*
TKN	GL292	GLRptWRTR	Balance Sheet	GRANTED	A,C,D,I,J,M,N,P,R,S,V	*ALL_ACCESS*

Policy - User Violation Report (LS and Landmark)



Segregation of Duties Report
Production - LS3SERVER - Profile: APS
Policy - User

Data as of: 2018-03-27 09:24:14.0
Display All Conditional Logic

Category: **ASSET MANAGEMENT**

Policy: 001 ★★★★★

Description: 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)

Security Violations for User: **Angie Davis (adavis)**

Group 1:
AM145 (TKN) or AM40.1 (TKN) or AM41.1 (TKN) or GL120 (TKN)

Type	Object	Security Class	Description	Rule	Avail FC	Prediction
TKN	AM145	ACCapitalization	Mass Disposals	GRANTED	A,C,D,I,J,M,N,P,R,S,V	*ALL_ACCESS*
TKN	AM40.1	AMProcessing	Disposals	GRANTED	A,D,I,N,P,Q,R	*A,I*
TKN	AM41.1	AMProcessing	Reinstate Disposed Assets	GRANTED	A,D,I,N,P,R	*ALL_ACCESS*

Group 2:
AM270 (TKN) or GL45.1 (TKN) or GL45.2 (TKN)

Type	Object	Security Class	Description	Rule	Avail FC	Prediction
TKN	AM270	AMAnalysis	Account Balance Report	GRANTED	A,C,D,I,J,M,N,P,R,S,V	*ALL_ACCESS*
TKN	GL45.1	FSS	Journal Control	GRANTED	+,-,B,C,F,I	*ALL_ACCESS*

Security Violations for User: **Bill Thomas (bthomas)**

Security Violations for User: **Frank Nelson (fnelson)**

Security Violations for User: **Helen Roberts (hroberts)**

Security Violations for User: **Hal Rogers (hrogers)**

Security Violations for User: **Lawson Lawson (lawson)**

Security Violations for User: **Mike Nitka (mnitka)**

Security Violations for User: **Sammy Christian (schristian)**

Security Violations for User: **Sarah Miller (smiller)**

Policy: 002 ★★★★★

Description: Investigate Discrepancies or Issues - Fixed Assets conflicts with Initiate Disposal of Fixed Assets. If one individual has responsibility for more than one of these functions, that individual could misappropriate assets and conceal the misappropriation. (13-10)

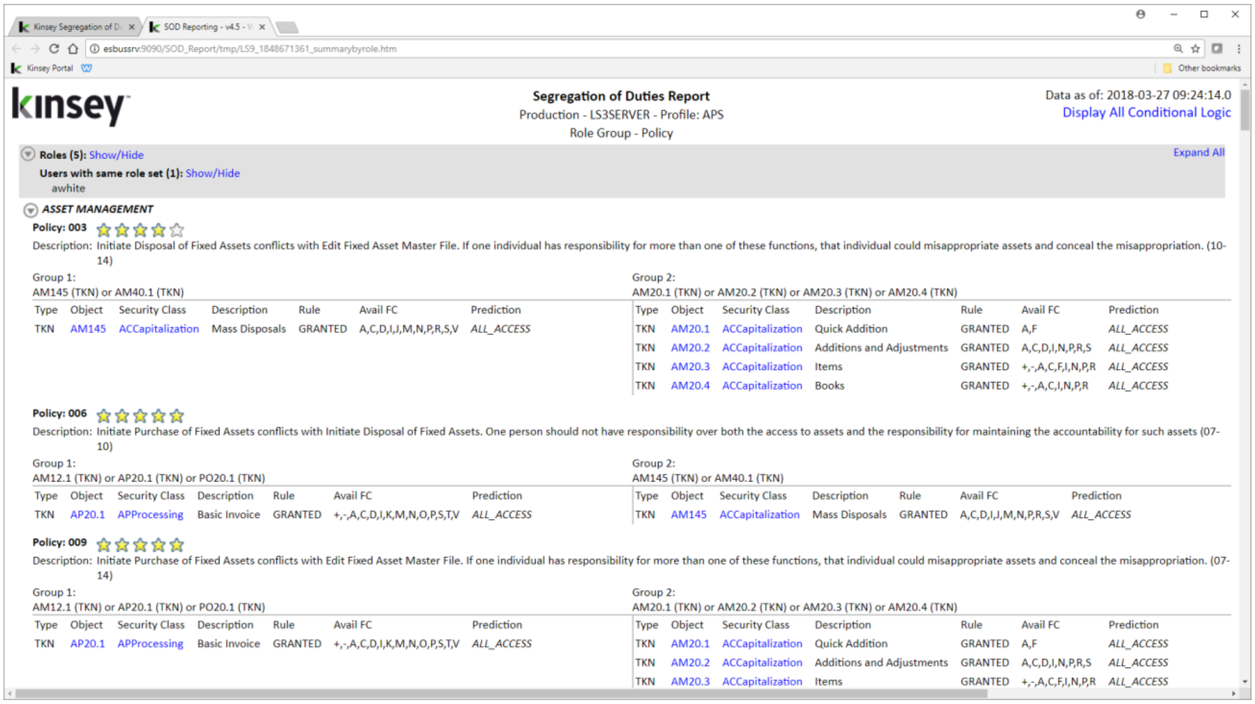
Security Violations for User: **Angie Davis (adavis)**

Security Violations for User: **Bill Thomas (bthomas)**

Security Violations for User: **Frank Nelson (fnelson)**

Security Violations for User: **Hal Rogers (hrogers)**

Role Group-Policy Violation Report (LS and Landmark)



Segregation of Duties Report
Production - LS3SERVER - Profile: APS
Role Group - Policy

Data as of: 2018-03-27 09:24:14.0
Display All Conditional Logic

Roles (5): Show/Hide
Users with same role set (1): Show/Hide
awhite

Expand All

ASSET MANAGEMENT

Policy: 003 ★★★★☆

Description: 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)

Group 1:
AM145 (TKN) or AM40.1 (TKN)

Type	Object	Security Class	Description	Rule	Avail FC	Prediction
TKN	AM145	ACCapitalization	Mass Disposals	GRANTED	A,C,D,I,J,M,N,P,R,S,V	*ALL_ACCESS*

Group 2:
AM20.1 (TKN) or AM20.2 (TKN) or AM20.3 (TKN) or AM20.4 (TKN)

Type	Object	Security Class	Description	Rule	Avail FC	Prediction
TKN	AM20.1	ACCapitalization	Quick Addition	GRANTED	A,F	*ALL_ACCESS*
TKN	AM20.2	ACCapitalization	Additions and Adjustments	GRANTED	A,C,D,I,N,P,R,S	*ALL_ACCESS*
TKN	AM20.3	ACCapitalization	Items	GRANTED	+,-,A,C,F,I,N,P,R	*ALL_ACCESS*
TKN	AM20.4	ACCapitalization	Books	GRANTED	+,-,A,C,I,N,P,R	*ALL_ACCESS*

Policy: 006 ★★★★★

Description: Initiate Purchase of Fixed Assets conflicts with Initiate Disposal of Fixed Assets. One person should not have responsibility over both the access to assets and the responsibility for maintaining the accountability for such assets (07-10)

Group 1:
AM12.1 (TKN) or AP20.1 (TKN) or PO20.1 (TKN)

Type	Object	Security Class	Description	Rule	Avail FC	Prediction
TKN	AP20.1	APProcessing	Basic Invoice	GRANTED	+,-,A,C,D,I,K,M,N,O,P,S,T,V	*ALL_ACCESS*

Group 2:
AM145 (TKN) or AM40.1 (TKN)

Type	Object	Security Class	Description	Rule	Avail FC	Prediction
TKN	AM145	ACCapitalization	Mass Disposals	GRANTED	A,C,D,I,J,M,N,P,R,S,V	*ALL_ACCESS*

Policy: 009 ★★★★★

Description: Initiate Purchase 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. (07-14)

Group 1:
AM12.1 (TKN) or AP20.1 (TKN) or PO20.1 (TKN)

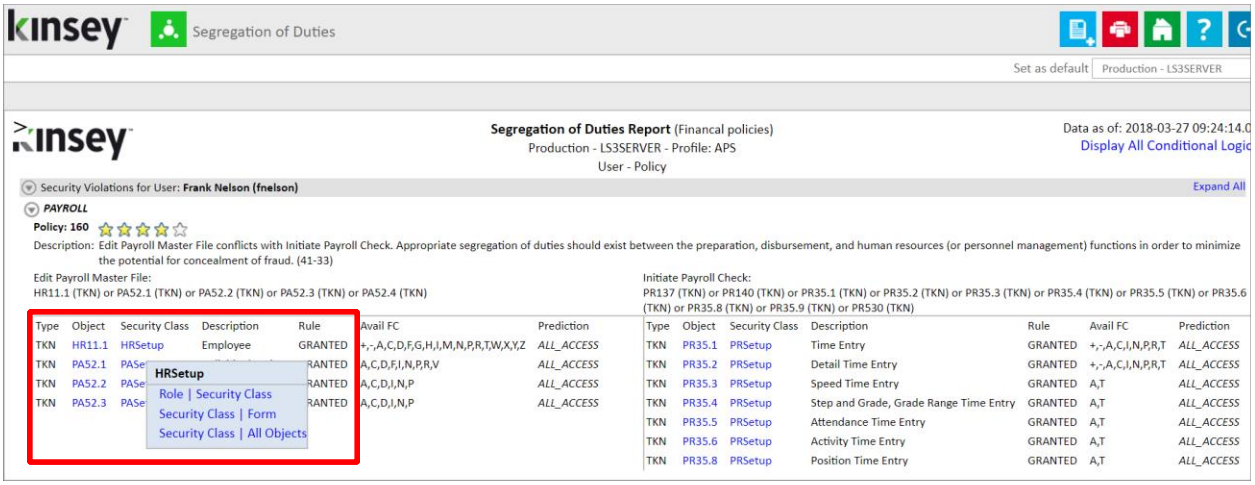
Type	Object	Security Class	Description	Rule	Avail FC	Prediction
TKN	AP20.1	APProcessing	Basic Invoice	GRANTED	+,-,A,C,D,I,K,M,N,O,P,S,T,V	*ALL_ACCESS*

Group 2:
AM20.1 (TKN) or AM20.2 (TKN) or AM20.3 (TKN) or AM20.4 (TKN)

Type	Object	Security Class	Description	Rule	Avail FC	Prediction
TKN	AM20.1	ACCapitalization	Quick Addition	GRANTED	A,F	*ALL_ACCESS*
TKN	AM20.2	ACCapitalization	Additions and Adjustments	GRANTED	A,C,D,I,N,P,R,S	*ALL_ACCESS*
TKN	AM20.3	ACCapitalization	Items	GRANTED	+,-,A,C,F,I,N,P,R	*ALL_ACCESS*

Drilling to Security Reports

If you are licensed for Kinsey's Lawson or Landmark Security reports the SoD reports provide the ability to drill into Security Class or Object details. Clicking on the hyperlinked objects will provide various report options.



Segregation of Duties Report (Financal policies)
Production - LS3SERVER - Profile: APS
User - Policy

Data as of: 2018-03-27 09:24:14.0
Display All Conditional Logic

Security Violations for User: **Frank Nelson (fnelson)**

Expand All

PAYROLL

Policy: 160 ★★★★☆

Description: Edit Payroll Master File conflicts with Initiate Payroll Check. Appropriate segregation of duties should exist between the preparation, disbursement, and human resources (or personnel management) functions in order to minimize the potential for concealment of fraud. (41-33)

Edit Payroll Master File:
HR11.1 (TKN) or PA52.1 (TKN) or PA52.2 (TKN) or PA52.3 (TKN) or PA52.4 (TKN)

Type	Object	Security Class	Description	Rule	Avail FC	Prediction
TKN	HR11.1	HRSetup	Employee	GRANTED	+,-,A,C,D,F,G,H,I,M,N,P,R,T,W,X,Y,Z	*ALL_ACCESS*
TKN	PA52.1	PASe		RANTED	A,C,D,F,I,N,P,R,V	*ALL_ACCESS*
TKN	PA52.2	PASe		RANTED	A,C,D,I,N,P	*ALL_ACCESS*
TKN	PA52.3	PASe		RANTED	A,C,D,I,N,P	*ALL_ACCESS*

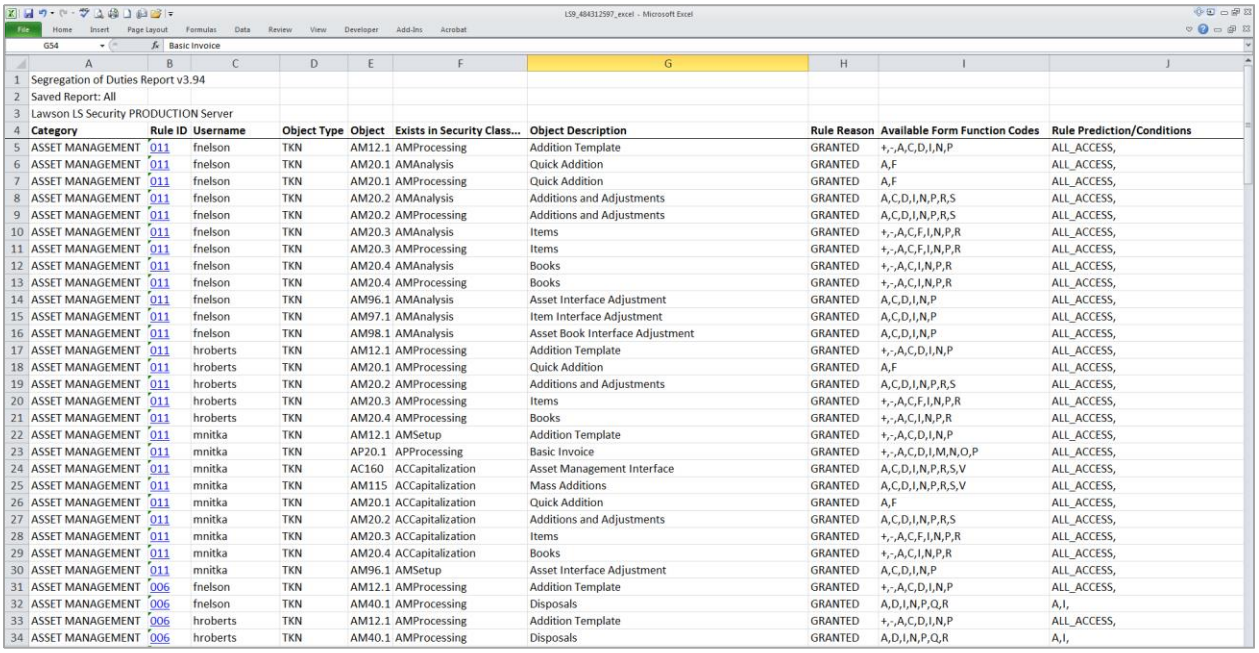
Initiate Payroll Check:
PR137 (TKN) or PR140 (TKN) or PR35.1 (TKN) or PR35.2 (TKN) or PR35.3 (TKN) or PR35.4 (TKN) or PR35.5 (TKN) or PR35.6 (TKN) or PR35.8 (TKN) or PR35.9 (TKN) or PR530 (TKN)

Type	Object	Security Class	Description	Rule	Avail FC	Prediction
TKN	PR35.1	PRSetup	Time Entry	GRANTED	+,-,A,C,I,N,P,R,T	*ALL_ACCESS*
TKN	PR35.2	PRSetup	Detail Time Entry	GRANTED	+,-,A,C,I,N,P,R,T	*ALL_ACCESS*
TKN	PR35.3	PRSetup	Speed Time Entry	GRANTED	A,T	*ALL_ACCESS*
TKN	PR35.4	PRSetup	Step and Grade, Grade Range Time Entry	GRANTED	A,T	*ALL_ACCESS*
TKN	PR35.5	PRSetup	Attendance Time Entry	GRANTED	A,T	*ALL_ACCESS*
TKN	PR35.6	PRSetup	Activity Time Entry	GRANTED	A,T	*ALL_ACCESS*
TKN	PR35.8	PRSetup	Position Time Entry	GRANTED	A,T	*ALL_ACCESS*

MS Excel Export (LS and Landmark)

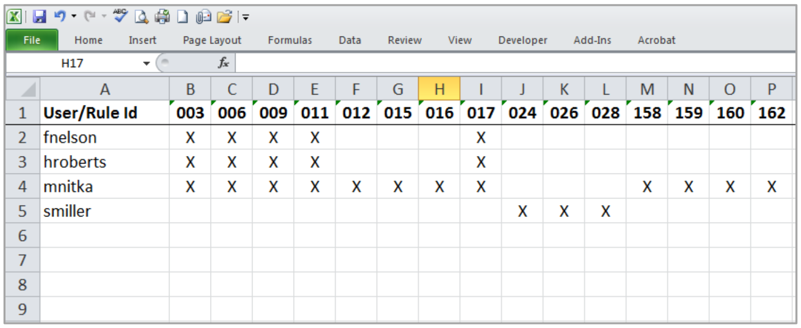
The Export version of the report creates 4 separate sheets. The first sheet consists of all violations by user and policy. You can use the data to sort or filter the results in any number of ways. The second sheet provides a high level overview of all policies violated by user. This is an easy way to evaluate the number of overall violations you have in your security model. The third sheet provides a list of the policies included in the report and the fourth sheet provides a legend of the Function Codes used in the report.

Excel Violation Report



	A	B	C	D	E	F	G	H	I	J
1	Segregation of Duties Report v3.94									
2	Saved Report: All									
3	Lawson LS Security PRODUCTION Server									
4	**Category**	**Rule ID**	**Username**	**Object Type**	**Object**	**Exists in Security Class...**	**Object Description**	**Rule Reason**	**Available Form Function Codes**	**Rule Prediction/Conditions**
5	ASSET MANAGEMENT	011	fnelson	TKN	AM12.1	AMProcessing	Addition Template	GRANTED	+,-,A,C,D,I,N,P	ALL_ACCESS,
6	ASSET MANAGEMENT	011	fnelson	TKN	AM20.1	AMAnalysis	Quick Addition	GRANTED	A,F	ALL_ACCESS,
7	ASSET MANAGEMENT	011	fnelson	TKN	AM20.1	AMProcessing	Quick Addition	GRANTED	A,F	ALL_ACCESS,
8	ASSET MANAGEMENT	011	fnelson	TKN	AM20.2	AMAnalysis	Additions and Adjustments	GRANTED	A,C,D,I,N,P,R,S	ALL_ACCESS,
9	ASSET MANAGEMENT	011	fnelson	TKN	AM20.2	AMProcessing	Additions and Adjustments	GRANTED	A,C,D,I,N,P,R,S	ALL_ACCESS,
10	ASSET MANAGEMENT	011	fnelson	TKN	AM20.3	AMAnalysis	Items	GRANTED	+,-,A,C,F,I,N,P,R	ALL_ACCESS,
11	ASSET MANAGEMENT	011	fnelson	TKN	AM20.3	AMProcessing	Items	GRANTED	+,-,A,C,F,I,N,P,R	ALL_ACCESS,
12	ASSET MANAGEMENT	011	fnelson	TKN	AM20.4	AMAnalysis	Books	GRANTED	+,-,A,C,I,N,P,R	ALL_ACCESS,
13	ASSET MANAGEMENT	011	fnelson	TKN	AM20.4	AMProcessing	Books	GRANTED	+,-,A,C,I,N,P,R	ALL_ACCESS,
14	ASSET MANAGEMENT	011	fnelson	TKN	AM96.1	AMAnalysis	Asset Interface Adjustment	GRANTED	A,C,D,I,N,P	ALL_ACCESS,
15	ASSET MANAGEMENT	011	fnelson	TKN	AM97.1	AMAnalysis	Item Interface Adjustment	GRANTED	A,C,D,I,N,P	ALL_ACCESS,
16	ASSET MANAGEMENT	011	fnelson	TKN	AM98.1	AMAnalysis	Asset Book Interface Adjustment	GRANTED	A,C,D,I,N,P	ALL_ACCESS,
17	ASSET MANAGEMENT	011	hroberts	TKN	AM12.1	AMProcessing	Addition Template	GRANTED	+,-,A,C,D,I,N,P	ALL_ACCESS,
18	ASSET MANAGEMENT	011	hroberts	TKN	AM20.1	AMProcessing	Quick Addition	GRANTED	A,F	ALL_ACCESS,
19	ASSET MANAGEMENT	011	hroberts	TKN	AM20.2	AMProcessing	Additions and Adjustments	GRANTED	A,C,D,I,N,P,R,S	ALL_ACCESS,
20	ASSET MANAGEMENT	011	hroberts	TKN	AM20.3	AMProcessing	Items	GRANTED	+,-,A,C,F,I,N,P,R	ALL_ACCESS,
21	ASSET MANAGEMENT	011	hroberts	TKN	AM20.4	AMProcessing	Books	GRANTED	+,-,A,C,I,N,P,R	ALL_ACCESS,
22	ASSET MANAGEMENT	011	mnitka	TKN	AM12.1	AMSetup	Addition Template	GRANTED	+,-,A,C,D,I,N,P	ALL_ACCESS,
23	ASSET MANAGEMENT	011	mnitka	TKN	AP20.1	APProcessing	Basic Invoice	GRANTED	+,-,A,C,D,I,M,N,O,P	ALL_ACCESS,
24	ASSET MANAGEMENT	011	mnitka	TKN	AC160	ACCapitalization	Asset Management Interface	GRANTED	A,C,D,I,N,P,R,S,V	ALL_ACCESS,
25	ASSET MANAGEMENT	011	mnitka	TKN	AM115	ACCapitalization	Mass Additions	GRANTED	A,C,D,I,N,P,R,S,V	ALL_ACCESS,
26	ASSET MANAGEMENT	011	mnitka	TKN	AM20.1	ACCapitalization	Quick Addition	GRANTED	A,F	ALL_ACCESS,
27	ASSET MANAGEMENT	011	mnitka	TKN	AM20.2	ACCapitalization	Additions and Adjustments	GRANTED	A,C,D,I,N,P,R,S	ALL_ACCESS,
28	ASSET MANAGEMENT	011	mnitka	TKN	AM20.3	ACCapitalization	Items	GRANTED	+,-,A,C,F,I,N,P,R	ALL_ACCESS,
29	ASSET MANAGEMENT	011	mnitka	TKN	AM20.4	ACCapitalization	Books	GRANTED	+,-,A,C,I,N,P,R	ALL_ACCESS,
30	ASSET MANAGEMENT	011	mnitka	TKN	AM96.1	AMSetup	Asset Interface Adjustment	GRANTED	A,C,D,I,N,P	ALL_ACCESS,
31	ASSET MANAGEMENT	006	fnelson	TKN	AM12.1	AMProcessing	Addition Template	GRANTED	+,-,A,C,D,I,N,P	ALL_ACCESS,
32	ASSET MANAGEMENT	006	fnelson	TKN	AM40.1	AMProcessing	Disposals	GRANTED	A,D,I,N,P,Q,R	A,I,
33	ASSET MANAGEMENT	006	hroberts	TKN	AM12.1	AMProcessing	Addition Template	GRANTED	+,-,A,C,D,I,N,P	ALL_ACCESS,
34	ASSET MANAGEMENT	006	hroberts	TKN	AM40.1	AMProcessing	Disposals	GRANTED	A,D,I,N,P,Q,R	A,I,

Violation grid



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	**User/Rule Id**	**003**	**006**	**009**	**011**	**012**	**015**	**016**	**017**	**024**	**026**	**028**	**158**	**159**	**160**	**162**
2	fnelson	X	X	X	X				X							
3	hroberts	X	X	X	X				X							
4	mnitka	X	X	X	X	X	X	X	X				X	X	X	X
5	smiller									X	X	X				
6																
7																
8																
9																

Notes: