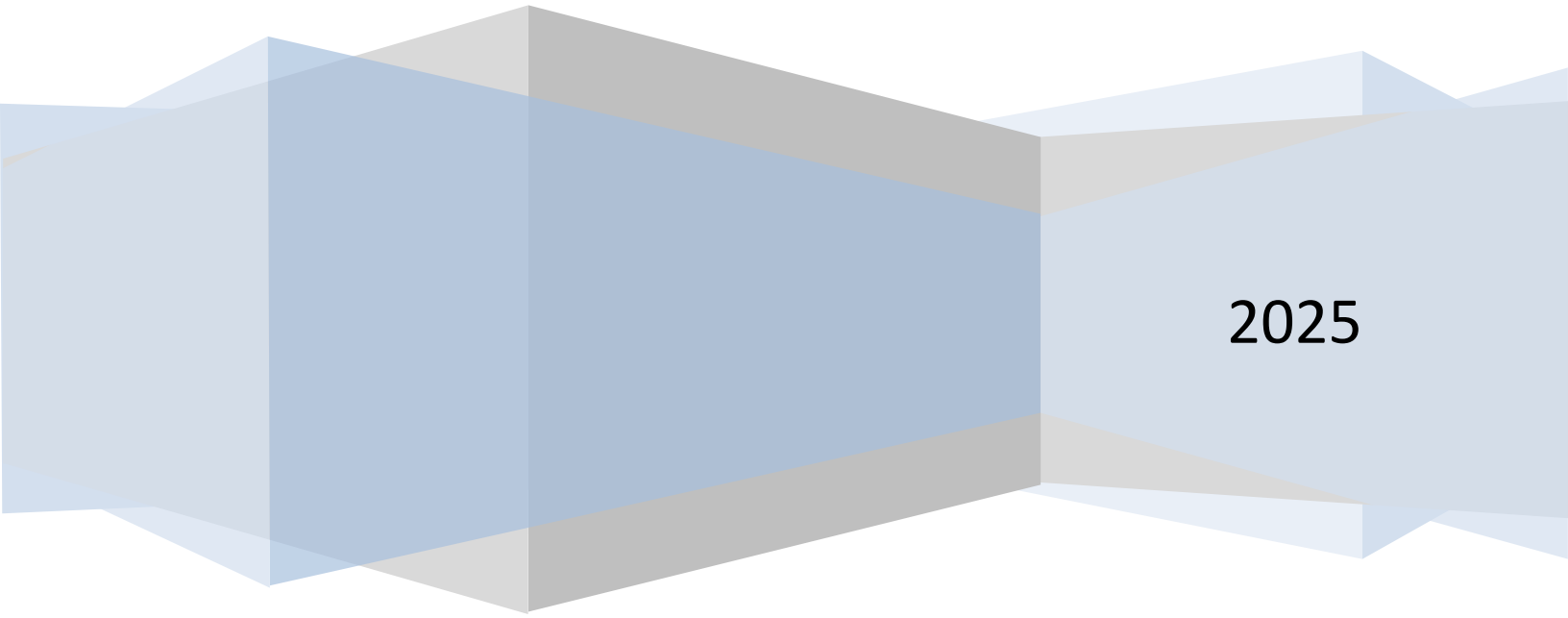
Segregation of Duties User Guide

Document contains instructions related to Segregation of Duties reporting



2025

Contents

Introduction 3
Getting Started 4
Logging in 4
Administration 5
Policy Maintenance 5
Reporting 6
Creating a New Report 7
Creating a Role Test Report 8
Editing an Existing Report 9
Mitigating a policy 10
Running a Saved Report 11
Actor (User) -Policy 12
Policy – Actor (User) 12
Role Group-Policy 12
Differences Report 12
Renaming a Report 12
Deleting a Report 12
Scheduling a Report 12
Historical Reports 14
Activating or Deactivating a Scheduled Report 15
Report Formats 16
User- Policy Violation Report 16
Role Group-Policy Violation Report 17
Drilling to Security Reports 18
MS Excel Export 19
Creating Mitigation using the Excel Upload 23
Assign or chancing a mitigation 23
Deleting a mitigation 23
Creating the mitigation upload file. 24
Uploading the mitigation changes. 25
Backing our your changes. 26

Introduction

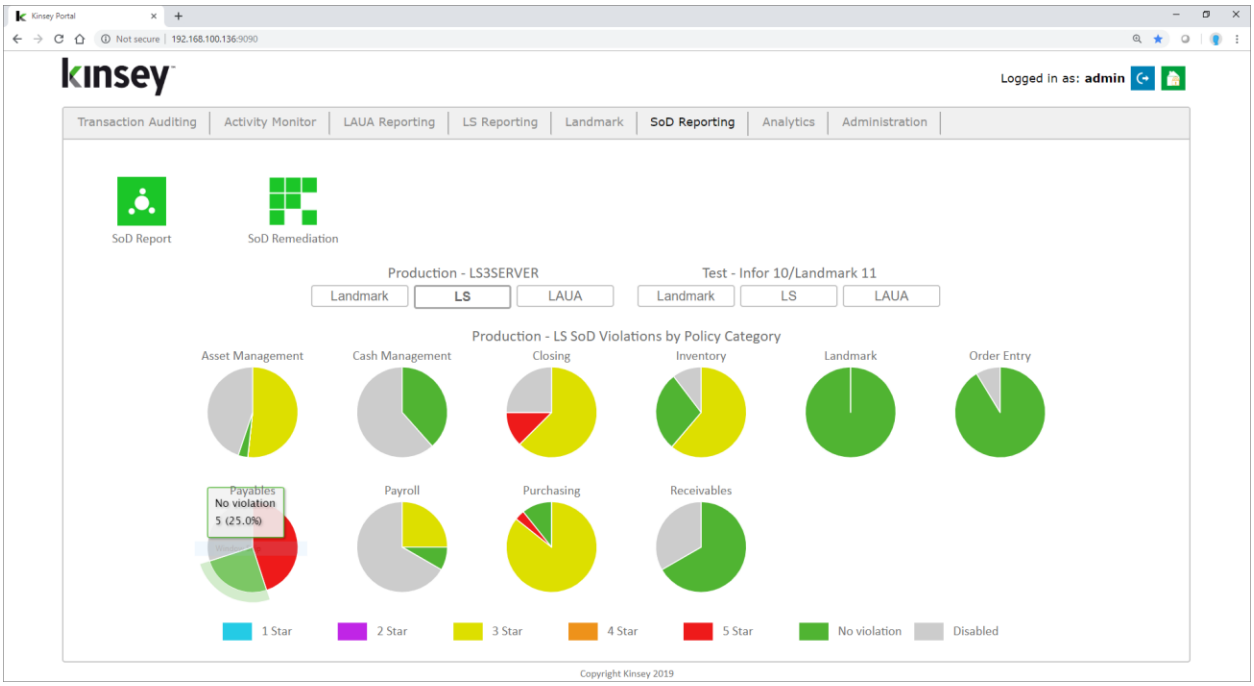
Kinsey's Segregation of Duties (SoD) Reporting is designed to examine Lawson S3 and CloudSuite/Landmark Security to determine if the proper checks and balances are being following in the respective security models. The delivered policies cover applications included in the Lawson and Landmark product suites are provided on a best efforts basis only and may not be complete or suitable for all organizations. 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. In some cases the application may report "false positives" for a possible violation where conditional or LPLlogic may actually restrict a users access. 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. The mitigation option allows you to flag any violated policy as allowable for a specific person and time period.

Features:

- Policies and rules are delivered for both Lawson S3 and CloudSuite (Landmark)
- Ability to add an unlimited number of policies and rules
- Ability to activate and rank policies individually
- Reports are available by User or by Policy
- Excel export options
- Differences Reporting
- Mitigation notes for policy violations

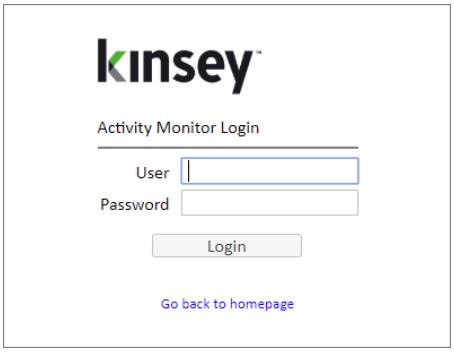
Getting Started

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.

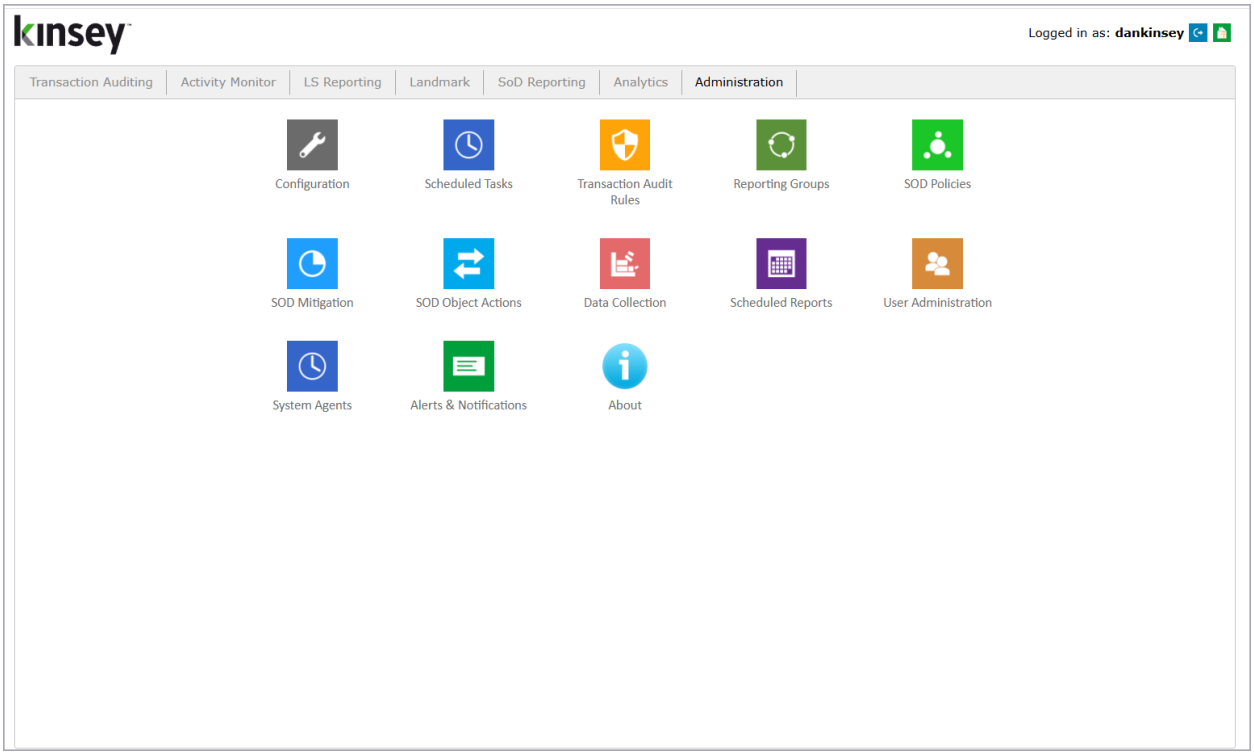


Logging in

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.



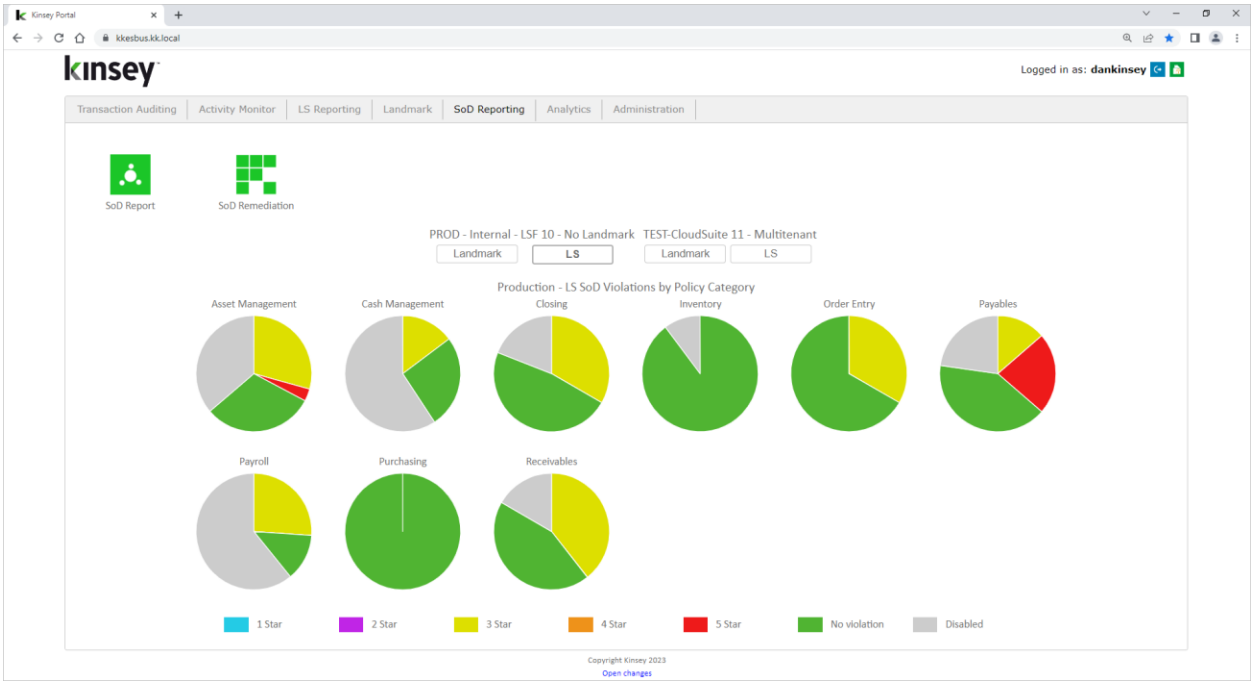
Administration



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 pie charts for up to 12 policy categories. By default the application will display charts for the LS Production environment with additional options LS Test, Landmark Production and Landmark Test environments.

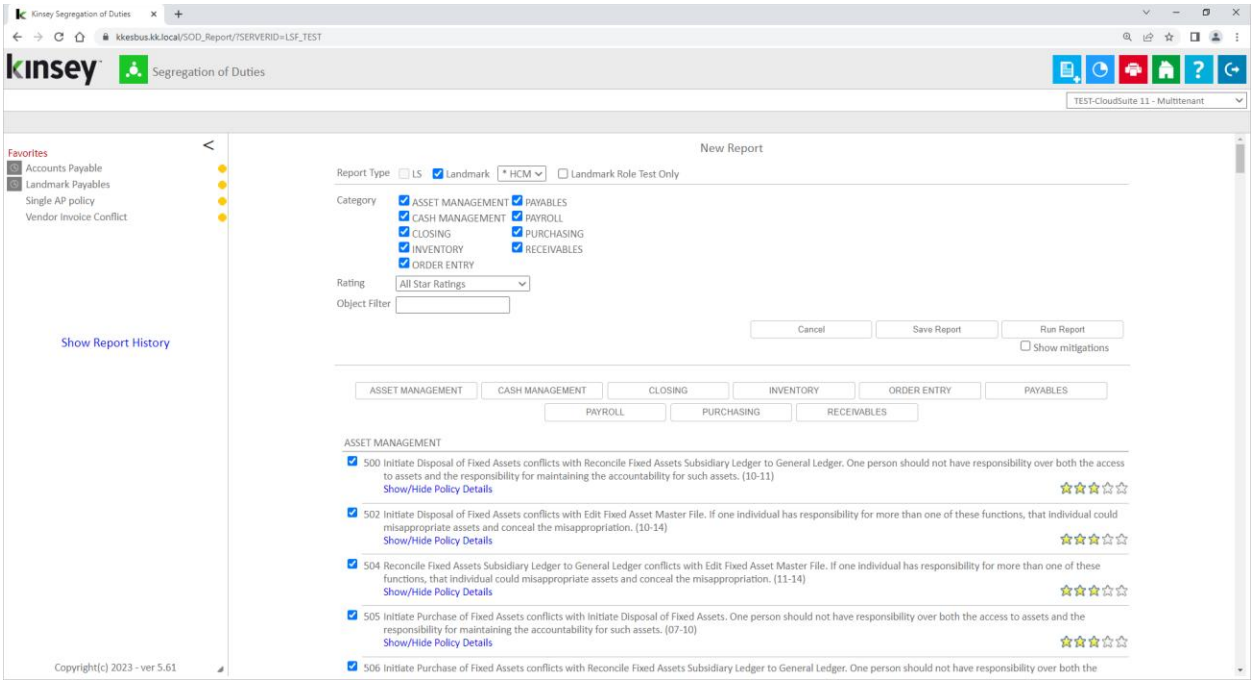
There are potentially 7 colors that could be displayed on each chart.

- 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 Infor 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



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 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.

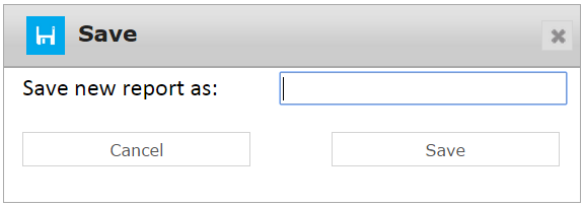
- User Violation Report – this report will show all violations for each User/Actor.
- Role Test Report – this report will report on violations for any Role or Role combinations.

To create a new SoD violation report use the Category, Level of Importance (star rating) and Object 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.
Rating:	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.
Object Filter:	The object filter will display all policies that include the object as part of the SoD rule definition entered. For example, if you want all policies that

pertain to vendor maintenance enter AP10.1 for S3 or Vendor for LMK in the Obect Filter field.

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.



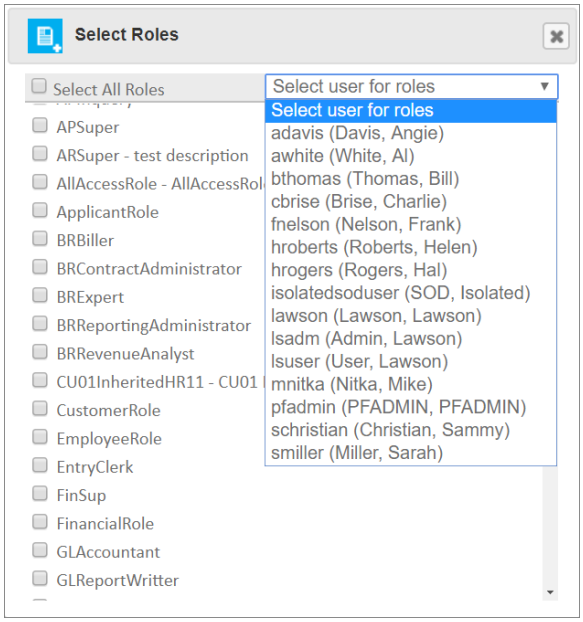
Note: the system does not store the Form filter or the Level of Importance with the report parameters, rather it stores the actual policies selected. If you edit an existing report you can revise your policy list by using the check box next to the policy number. See Editing a Report for more information

Creating a Role Test Report

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.

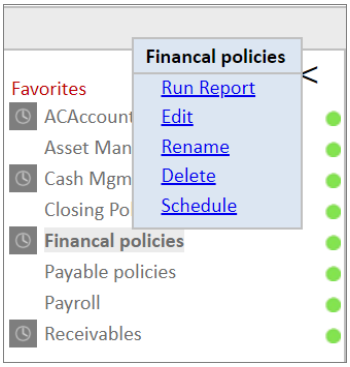
When the list of roles is displayed you can choose any combination of roles or select an existing user from the dropdown window. When you select a user the roles assigned to them will automatically be checked. You can then check any other role you might want to add to this user. When you are finished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

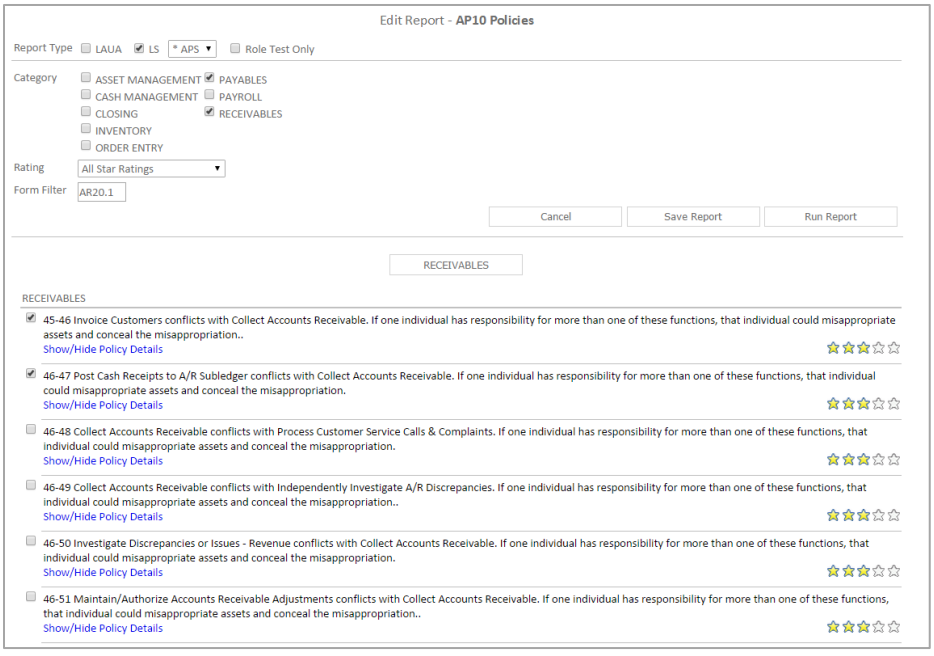
Editing an Existing Report

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.

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.



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.

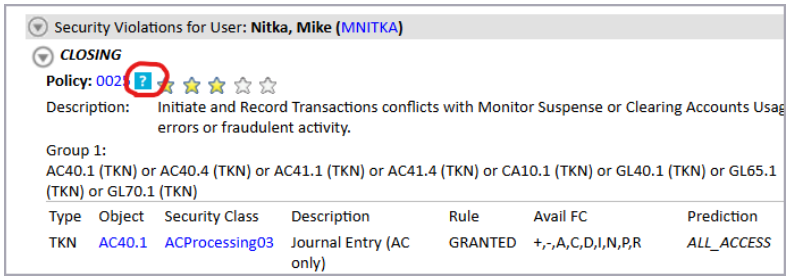
Mitigating a policy.

The mitigation option allows you to flag a policy as allowable for a specific user for a designated period of time. There are 3 options when assigning a mitigation.

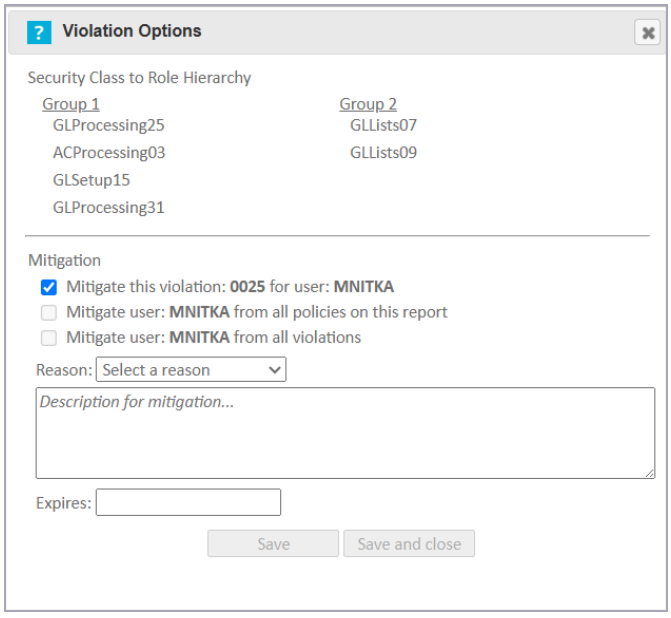
1. Specifically for the User and the policy violation selected
2. For the User and all policy violations included in the current report.
3. The All Violations option will mitigate any current or future polices for this user.

WARNING. Option 3 was put in primarly for administrators and technical support. If you assign ALL to a user any future policies will all be mitigated by default.

When the results are displayed for a user you can add a mitigation by clicking on the blue question mark icon next to the users name. Mitigation Reason Codes can be defined under the SoD Mitigation option on the Adminstration page. The description and expiration date are optional.

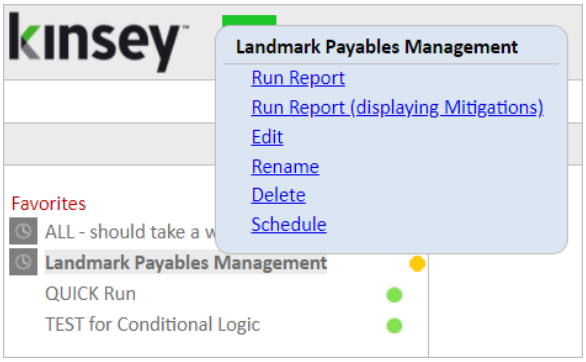


Selec t the mitigation type, select a reason code, enter and description if needed and set the optional Exipres date. Mitagations will automatically expire for a user after the date entered.



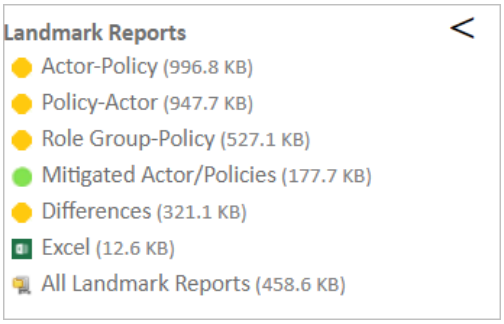
Running a Saved Report

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. You can run the report with or without diaplying existing mitigations. HTML reports that include mitigated policies will display with a watermark over the mitigated policy. If you run the report without mitigations you will have the option to display all mitigated policies on a separate report.



The color of the dot next to the report indicates the security model being checked. A green dot indicates the report is checking LS security 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.



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.

Actor (User) -Policy

This report provides a list of User's and the policies they are currently violating. (See page 16)

Policy – Actor (User)

This report provides a list of Policies and the User's in violation. Policy are grouped by SoD Category. (See page 17)

Role Group-Policy

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 17)

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.

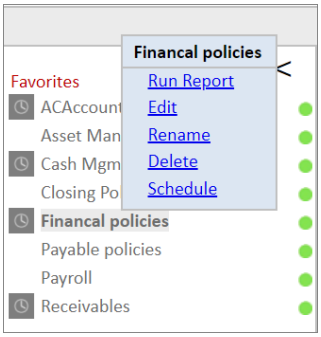
Deleting a Report

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.

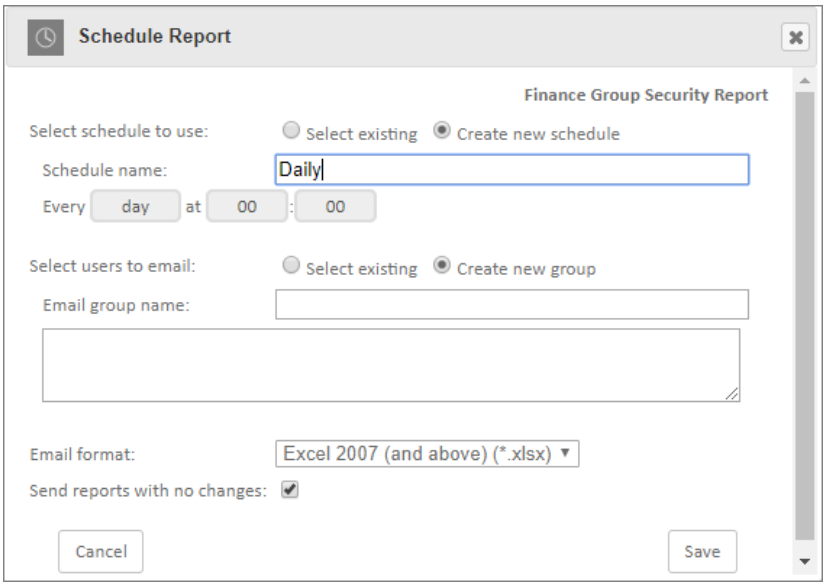
To schedule a report you must first create and save your report. Once the report displays under saved reports in the left navigation pane, click on the report name and select Schedule.



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).

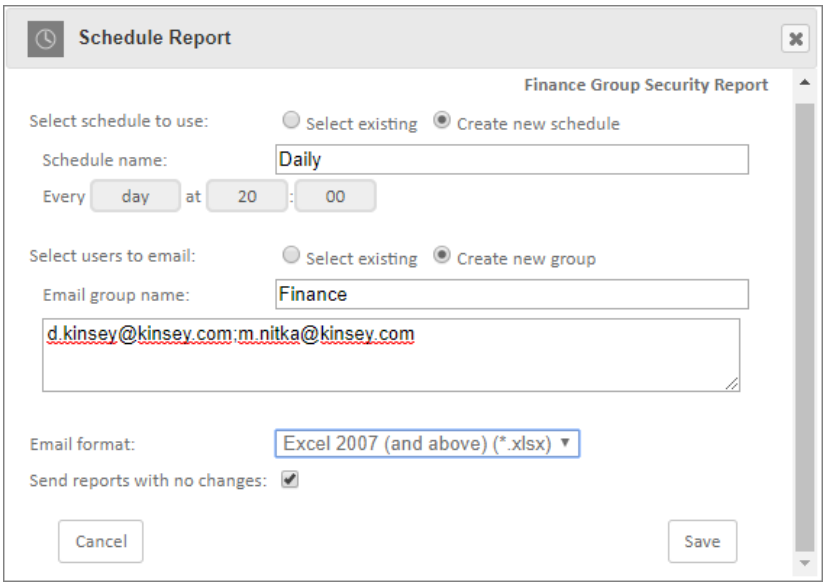
NOTE: The schedule must be enabled for the schedule to run. To enable a scheduled report refer to the Schedule Reports section of the Administrators Guide.

The scheduling screen allows you to setup new schedules or use existing schedules. Schedules can be set to run on various frequencies. 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.



Email format:

The export options are Excel or Adobe PDF

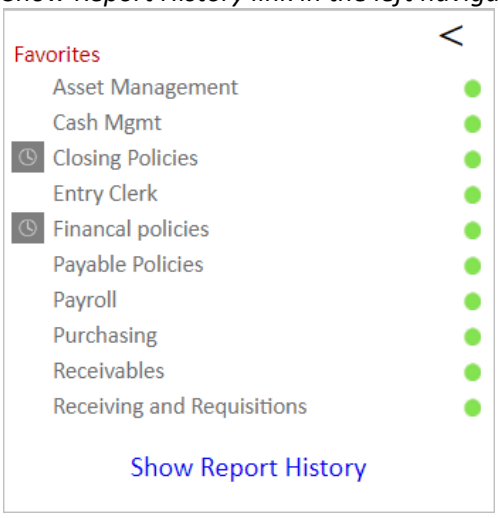
Send blank reports:

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.

Historical Reports

The application will retain a history of reports by date and time. To acess Historical Reports click on the Show Report History link in the left navigation pane under the saved reports.



A list of reports will be displayed in the center pane. Select a Job Number to view a list of reports and click on the version of the report you would like to view.

SOD Report History

Job Number	Report Name	Submitted By	Submitted On
000000944	Purchasing	dankinsey	8/15/2022 3:20PM
000000895	(on demand)	dankinsey	7/22/2022 9:55AM

File Name	Size
SOD_LS_000000895.zip	346.3 KB
SOD_LS_000000895_excel.xlsx	12.7 KB
SOD_LS_000000895_mitigatedrules.htm	184.4 KB
SOD_LS_000000895_sortedbyrule.htm	236.3 KB
SOD_LS_000000895_sortedbyuser.htm	242.2 KB
SOD_LS_000000895_summarybyrole.htm	243.9 KB

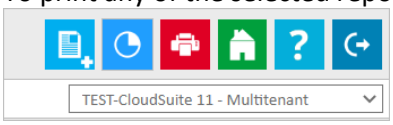
000000894	(on demand)	dankinsey	7/22/2022 9:46AM
000000893	(on demand)	dankinsey	7/22/2022 9:42AM
000000892	(on demand)	dankinsey	7/22/2022 9:42AM
000000891	(on demand)	dankinsey	7/22/2022 9:40AM
000000790	(on demand)	dankinsey	6/2/2022 8:28AM
000000763	Payable Policies	dankinsey	5/20/2022 9:53AM
000000762	(on demand)	dankinsey	5/20/2022 9:49AM

Activating or Deactivating a Scheduled Report

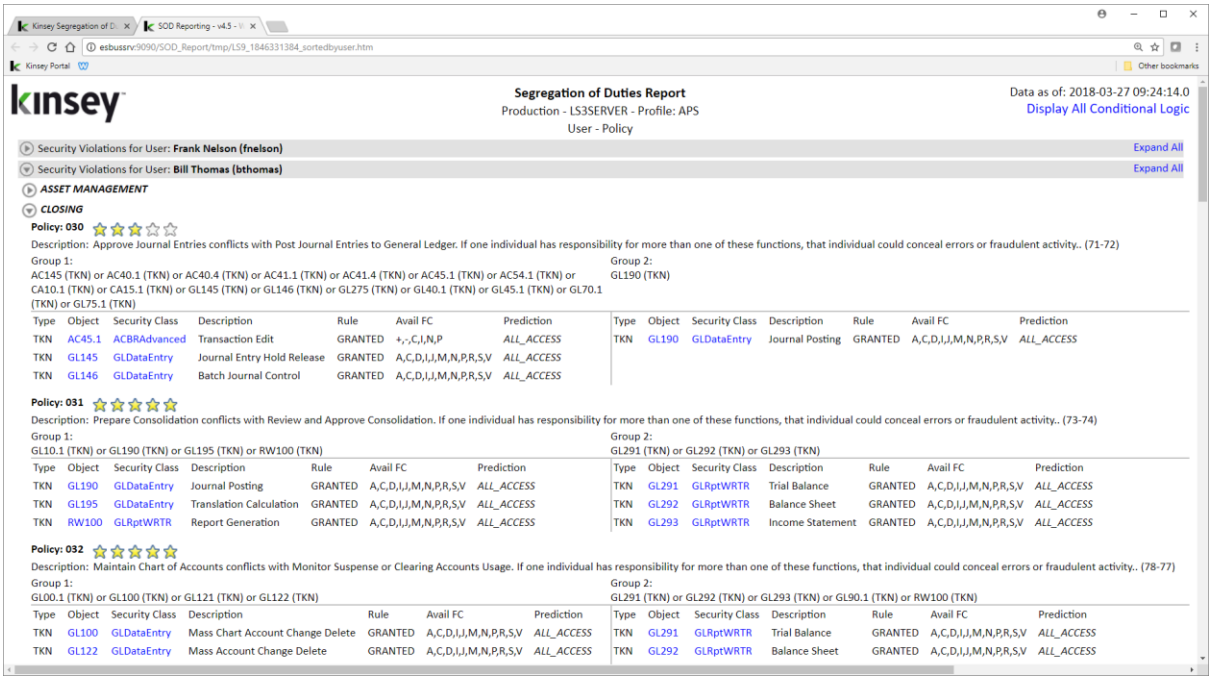
To change the activation status of a schedule you need to access the Schedule Reports option on the Administration tab. Refer to Scheduled Reports in the Kinsey Admin Guide for details on how to manage scheduled reports.

Report Formats

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



User- Policy Violation Report



kinsey

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)

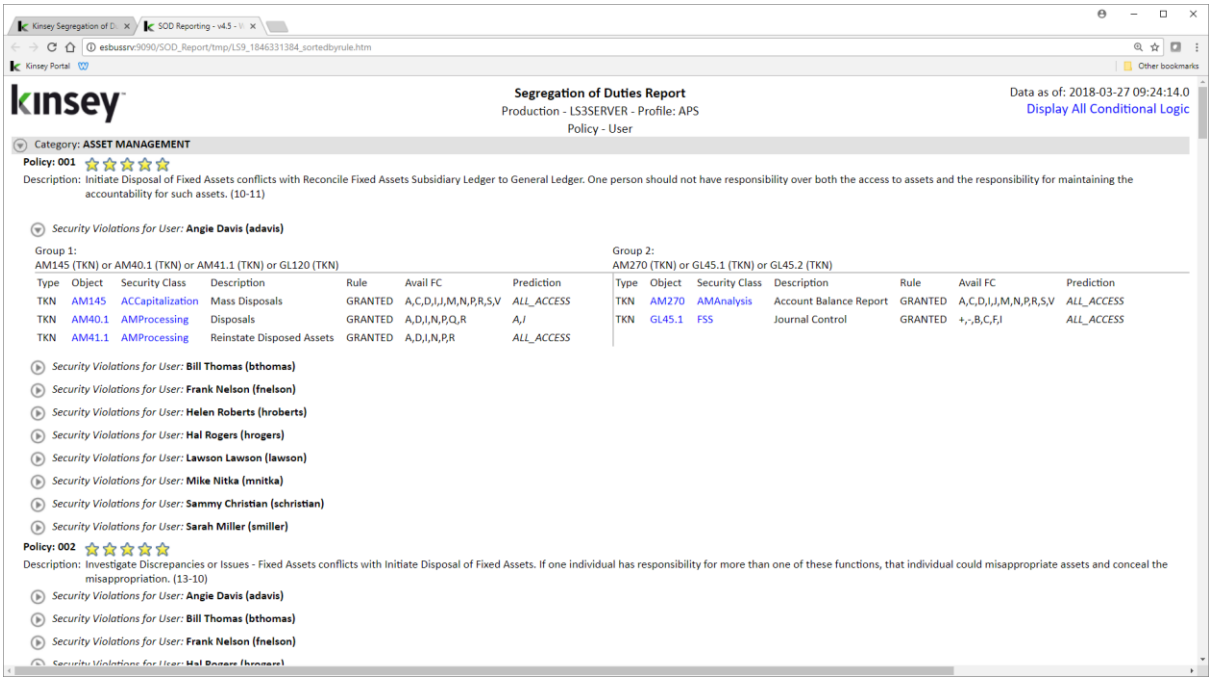
Group 1:
GL00.1 (TKN) or GL100 (TKN) or GL121 (TKN) or GL122 (TKN)

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



kinsey

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*

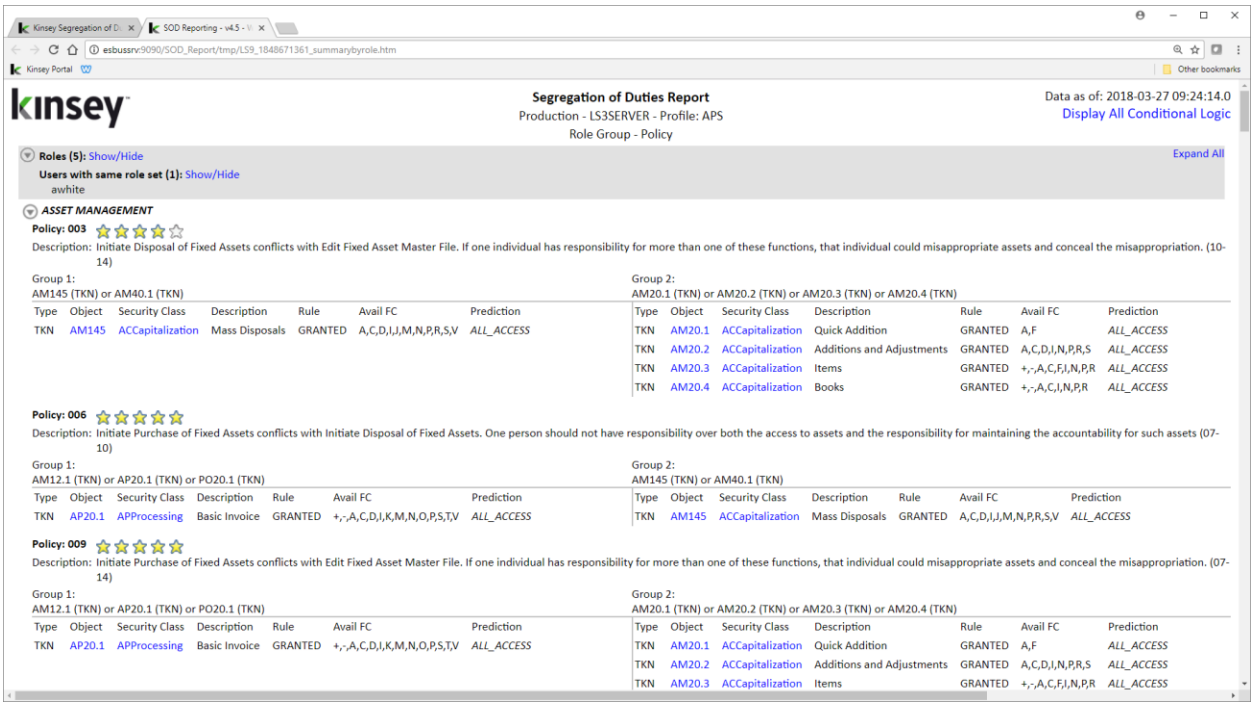
Security Violations for User: **Bill Thomas (bthomas)**
Security Violations for User: **Frank Nelson (fnelson)**
Security Violations for User: **Helen Roberts (hroberts)**
Security Violations for User: **Hal Rogers (hrogers)**
Security Violations for User: **Lawson Lawson (lawson)**
Security Violations 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)**

Role Group-Policy Violation Report



kinsey

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
Expand All
Users with same role set (1): Show/Hide
awhite

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)

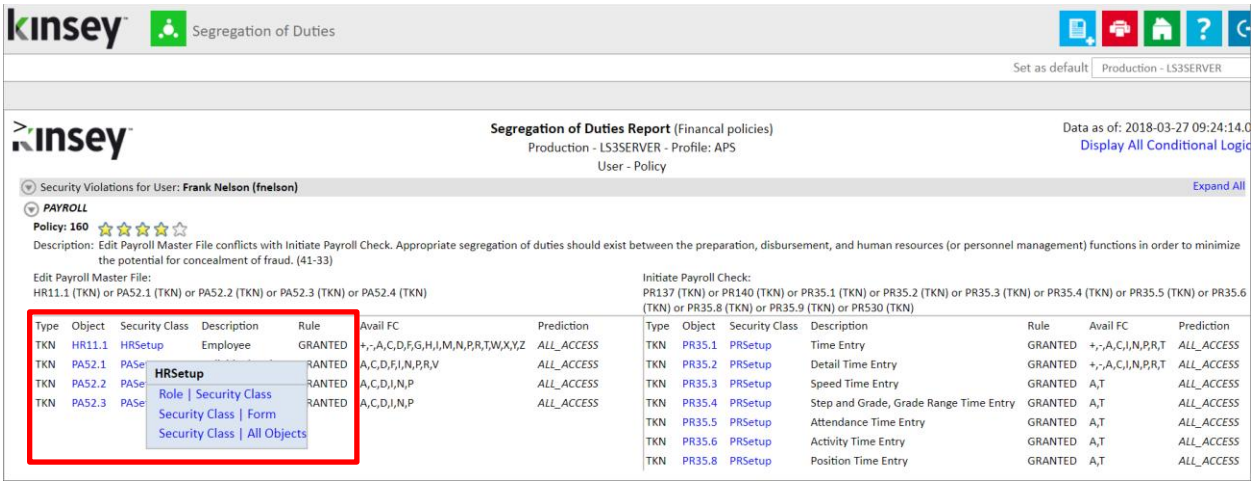
Type	Object	Security Class	Description	Rule	Avail FC	Prediction
TKN	AP20.1	APProcessing	Basic Invoice	GRANTED	+,-,A,C,D,I,K,M,N,O,P,S,T,V	*ALL_ACCESS*

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.



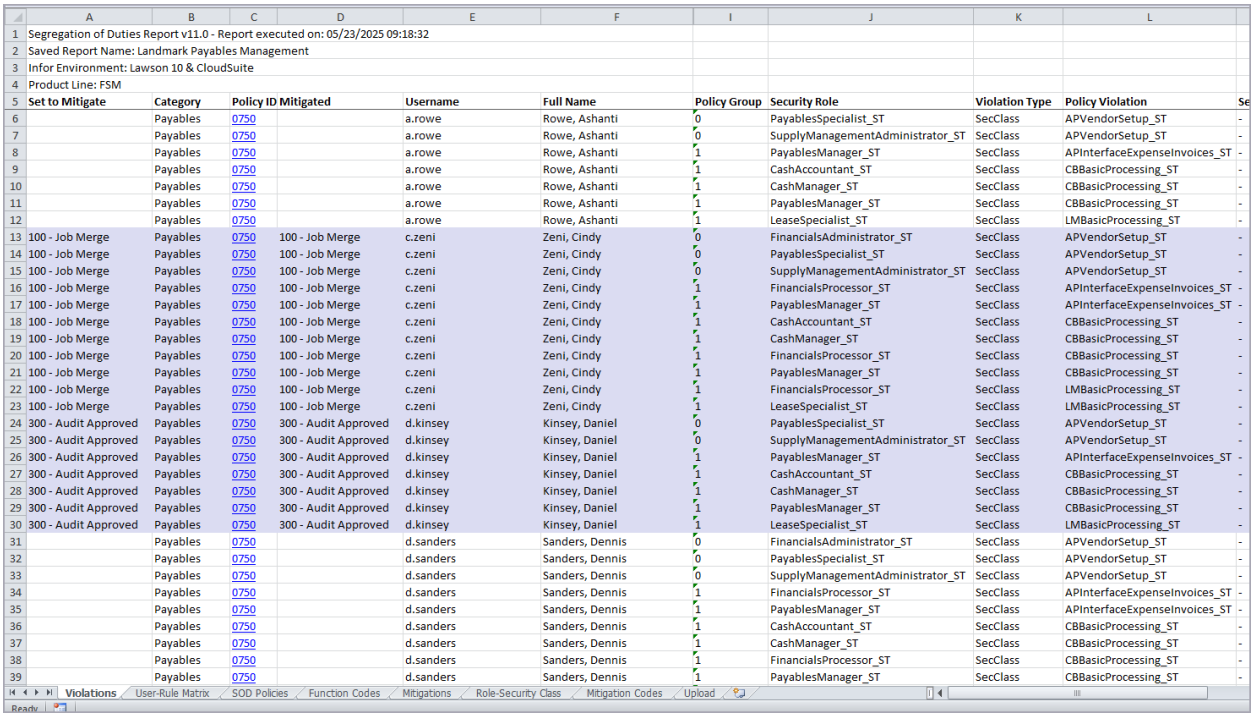
You can also drill to security reports more specific to the violation being displayed. By clicking on the User ID you will get a set of User specific reports and clicking on the Policy # will provide a report of just the Roles causing this violation.

MS Excel Export

The Export version of the report creates 8 separate sheets.

1. Sheet one- **Violations** - is a list of all violations by user and policy. You can use the data to sort or filter the results in any number of ways or to mitigate user policies.
2. Sheet 2 – **User-Role Matrix** - provides a matrix of user/policy violations. This is an easy way to evaluate the number of overall violations you have in your security model.
3. Sheet 3 - **SOD Policies** - displays a list of the policies included in the report
4. Sheet 4 – **FC-Actions** provides a legend of the Function Codes (S3) or Actions (LMK) used in the report.
5. Sheet 5 – **Mitigations** - is an export of all current SoD mitigations.
6. Sheet 6 - Role-Security Class – includes a complete list of all Roles connected to objects on this report and the specific Security Classes found on the report.
7. Sheet 7 – Mitigation Codes – include a list of codes used on the report
8. Sheet 8 – this provides the option to create an upload file for any mitigation added to this report.

Sheet 1: Violation Report



	A	B	C	D	E	F	I	J	K	L	
1	Segregation of Duties Report v11.0 - Report executed on: 05/23/2025 09:18:32										
2	Saved Report Name: Landmark Payables Management										
3	Infor Environment: Lawson 10 & CloudSuite										
4	Product Line: FSM										
5	**Set to Mitigate**	**Category**	**Policy ID**	**Mitigated**	**Username**	**Full Name**	**Policy Group**	**Security Role**	**Violation Type**	**Policy Violation**	**Se**
6		Payables	0750		a.rowe	Rowe, Ashanti	0	PayablesSpecialist_ST	SecClass	APVendorSetup_ST	-
7		Payables	0750		a.rowe	Rowe, Ashanti	0	SupplyManagementAdministrator_ST	SecClass	APVendorSetup_ST	-
8		Payables	0750		a.rowe	Rowe, Ashanti	1	PayablesManager_ST	SecClass	APInterfaceExpenseInvoices_ST	-
9		Payables	0750		a.rowe	Rowe, Ashanti	1	CashAccountant_ST	SecClass	CBBasicProcessing_ST	-
10		Payables	0750		a.rowe	Rowe, Ashanti	1	CashManager_ST	SecClass	CBBasicProcessing_ST	-
11		Payables	0750		a.rowe	Rowe, Ashanti	1	PayablesManager_ST	SecClass	CBBasicProcessing_ST	-
12		Payables	0750		a.rowe	Rowe, Ashanti	1	LeaseSpecialist_ST	SecClass	LMBasicProcessing_ST	-
13	100 - Job Merge	Payables	0750	100 - Job Merge	c.zeni	Zeni, Cindy	0	FinancialsAdministrator_ST	SecClass	APVendorSetup_ST	-
14	100 - Job Merge	Payables	0750	100 - Job Merge	c.zeni	Zeni, Cindy	0	PayablesSpecialist_ST	SecClass	APVendorSetup_ST	-
15	100 - Job Merge	Payables	0750	100 - Job Merge	c.zeni	Zeni, Cindy	0	SupplyManagementAdministrator_ST	SecClass	APVendorSetup_ST	-
16	100 - Job Merge	Payables	0750	100 - Job Merge	c.zeni	Zeni, Cindy	1	FinancialsProcessor_ST	SecClass	APInterfaceExpenseInvoices_ST	-
17	100 - Job Merge	Payables	0750	100 - Job Merge	c.zeni	Zeni, Cindy	1	PayablesManager_ST	SecClass	APInterfaceExpenseInvoices_ST	-
18	100 - Job Merge	Payables	0750	100 - Job Merge	c.zeni	Zeni, Cindy	1	CashAccountant_ST	SecClass	CBBasicProcessing_ST	-
19	100 - Job Merge	Payables	0750	100 - Job Merge	c.zeni	Zeni, Cindy	1	CashManager_ST	SecClass	CBBasicProcessing_ST	-
20	100 - Job Merge	Payables	0750	100 - Job Merge	c.zeni	Zeni, Cindy	1	FinancialsProcessor_ST	SecClass	CBBasicProcessing_ST	-
21	100 - Job Merge	Payables	0750	100 - Job Merge	c.zeni	Zeni, Cindy	1	PayablesManager_ST	SecClass	CBBasicProcessing_ST	-
22	100 - Job Merge	Payables	0750	100 - Job Merge	c.zeni	Zeni, Cindy	1	FinancialsProcessor_ST	SecClass	LMBasicProcessing_ST	-
23	100 - Job Merge	Payables	0750	100 - Job Merge	c.zeni	Zeni, Cindy	1	LeaseSpecialist_ST	SecClass	LMBasicProcessing_ST	-
24	300 - Audit Approved	Payables	0750	300 - Audit Approved	d.kinsey	Kinsey, Daniel	0	PayablesSpecialist_ST	SecClass	APVendorSetup_ST	-
25	300 - Audit Approved	Payables	0750	300 - Audit Approved	d.kinsey	Kinsey, Daniel	0	SupplyManagementAdministrator_ST	SecClass	APVendorSetup_ST	-
26	300 - Audit Approved	Payables	0750	300 - Audit Approved	d.kinsey	Kinsey, Daniel	1	PayablesManager_ST	SecClass	APInterfaceExpenseInvoices_ST	-
27	300 - Audit Approved	Payables	0750	300 - Audit Approved	d.kinsey	Kinsey, Daniel	1	CashAccountant_ST	SecClass	CBBasicProcessing_ST	-
28	300 - Audit Approved	Payables	0750	300 - Audit Approved	d.kinsey	Kinsey, Daniel	1	CashManager_ST	SecClass	CBBasicProcessing_ST	-
29	300 - Audit Approved	Payables	0750	300 - Audit Approved	d.kinsey	Kinsey, Daniel	1	PayablesManager_ST	SecClass	CBBasicProcessing_ST	-
30	300 - Audit Approved	Payables	0750	300 - Audit Approved	d.kinsey	Kinsey, Daniel	1	LeaseSpecialist_ST	SecClass	LMBasicProcessing_ST	-
31		Payables	0750		d.sanders	Sanders, Dennis	0	FinancialsAdministrator_ST	SecClass	APVendorSetup_ST	-
32		Payables	0750		d.sanders	Sanders, Dennis	0	PayablesSpecialist_ST	SecClass	APVendorSetup_ST	-
33		Payables	0750		d.sanders	Sanders, Dennis	0	SupplyManagementAdministrator_ST	SecClass	APVendorSetup_ST	-
34		Payables	0750		d.sanders	Sanders, Dennis	1	FinancialsProcessor_ST	SecClass	APInterfaceExpenseInvoices_ST	-
35		Payables	0750		d.sanders	Sanders, Dennis	1	PayablesManager_ST	SecClass	APInterfaceExpenseInvoices_ST	-
36		Payables	0750		d.sanders	Sanders, Dennis	1	CashAccountant_ST	SecClass	CBBasicProcessing_ST	-
37		Payables	0750		d.sanders	Sanders, Dennis	1	CashManager_ST	SecClass	CBBasicProcessing_ST	-
38		Payables	0750		d.sanders	Sanders, Dennis	1	FinancialsProcessor_ST	SecClass	CBBasicProcessing_ST	-
39		Payables	0750		d.sanders	Sanders, Dennis	1	PayablesManager_ST	SecClass	CBBasicProcessing_ST	-

Violations | User-Role Matrix | SOD Policies | Function Codes | Mitigations | Role-Security Class | Mitigation Codes | Upload

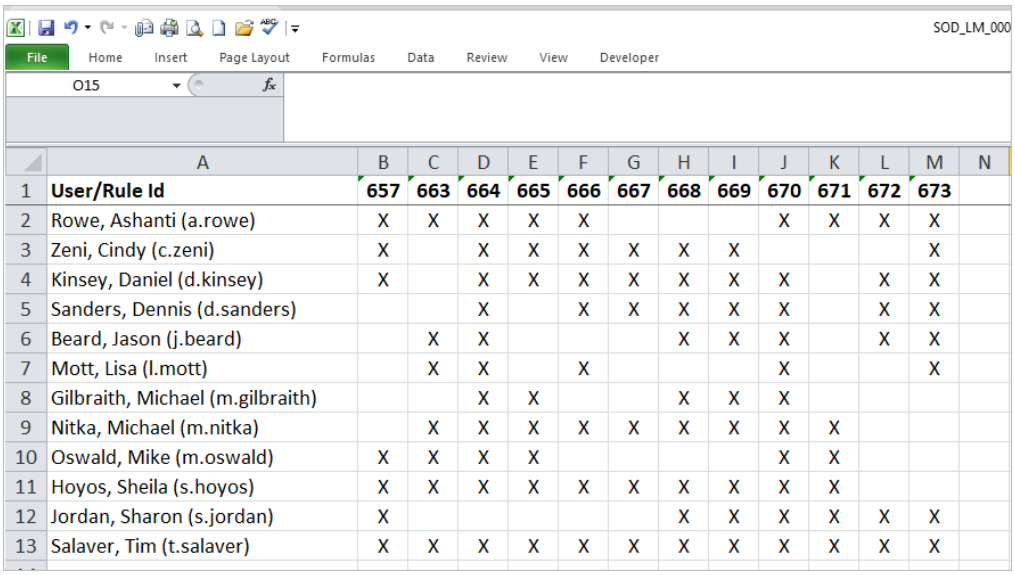
Ready

This is an example of a Landmark SoD report for the Payables policy 750. By looking at lines 6 through 13 I can see that Ashanti Rowe as access to 7 Roles and 4 unique security classes defined in the rule. Two security class are in group 0 and 5 security classes are in group 1.

Rules are built to check for conflicting objects between 2 groups (0 and 1). The application will flag the user as violating the policy if they have access to atleast 1 object in both groups. For rules built at the Token or Business Class level the application only considers there to be a violation if the users has more than inquiry only access.

If the report is run to include mitigations they will be displayed and highlighted in purple.

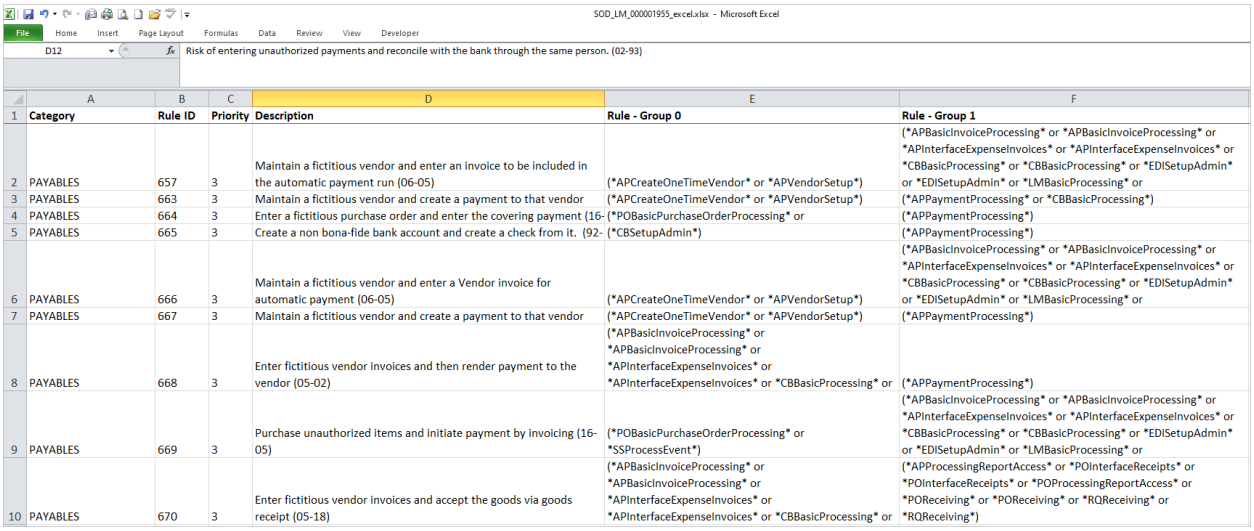
Sheet 2: User-Rule Matrix



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	**User/Rule Id**	**657**	**663**	**664**	**665**	**666**	**667**	**668**	**669**	**670**	**671**	**672**	**673**	
2	Rowe, Ashanti (a.rowe)	X	X	X	X	X				X	X	X	X	
3	Zeni, Cindy (c.zeni)	X		X	X	X	X	X	X				X	
4	Kinsey, Daniel (d.kinsey)	X		X	X	X	X	X	X	X		X	X	
5	Sanders, Dennis (d.sanders)			X		X	X	X	X	X		X	X	
6	Beard, Jason (j.beard)		X	X				X	X	X		X	X	
7	Mott, Lisa (l.mott)		X	X		X				X			X	
8	Gilbraith, Michael (m.gilbraith)			X	X			X	X	X				
9	Nitka, Michael (m.nitka)		X	X	X	X	X	X	X	X	X			
10	Oswald, Mike (m.oswald)	X	X	X	X					X	X			
11	Hoyos, Sheila (s.hoyos)	X	X	X	X	X	X	X	X	X	X			
12	Jordan, Sharon (s.jordan)	X						X	X	X	X	X	X	
13	Salaver, Tim (t.salaver)	X	X	X	X	X	X	X	X	X	X	X	X	

The ‘X’ indicates that a user violations a particular policy. When comparing this report to sheet 1, sheet 1 shows the detail of the objects the user has access too.

Sheet 3: SOD Rules



SOD_LM_00001955_excel.xlsx - Microsoft Excel

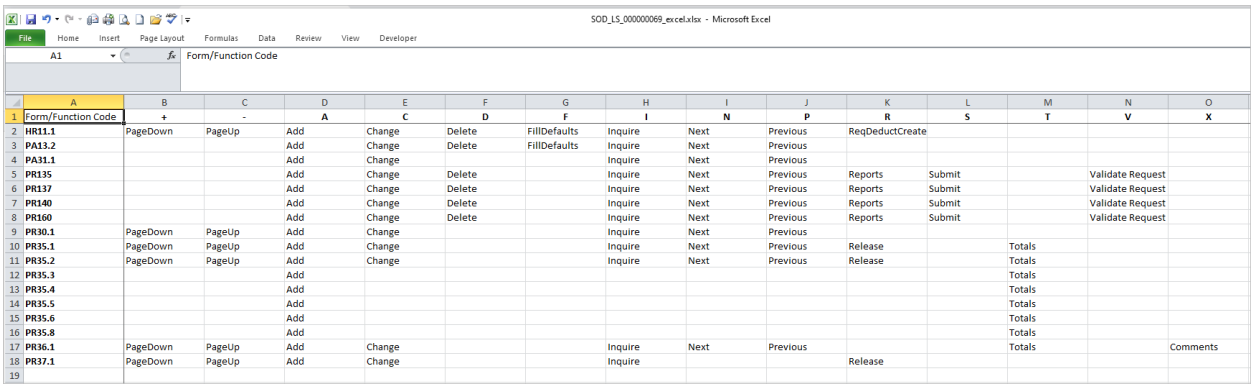
File Home Insert Page Layout Formulas Data Review View Developer

D12 — Risk of entering unauthorized payments and reconcile with the bank through the same person. (02-93)

	A	B	C	D	E	F
1	**Category**	**Rule ID**	**Priority**	**Description**	**Rule - Group 0**	**Rule - Group 1**
2	PAYABLES	657	3	Maintain a fictitious vendor and enter an invoice to be included in the automatic payment run (06-05)	(*APCreateOneTimeVendor* or *APVendorSetup*)	(*APBasicInvoiceProcessing* or *APBasicInvoiceProcessing* or *APInterfaceExpenseInvoices* or *APInterfaceExpenseInvoices* or *CBBasicProcessing* or *CBBasicProcessing* or *EDISetupAdmin* or *EDISetupAdmin* or *LMBasicProcessing* or
3	PAYABLES	663	3	Maintain a fictitious vendor and create a payment to that vendor	(*APCreateOneTimeVendor* or *APVendorSetup*)	(*APPaymentProcessing* or *CBBasicProcessing*)
4	PAYABLES	664	3	Enter a fictitious purchase order and enter the covering payment (16-	(*POBasicPurchaseOrderProcessing* or	(*APPaymentProcessing*)
5	PAYABLES	665	3	Create a non bona-fide bank account and create a check from it. (92-	(*CBSetupAdmin*)	(*APPaymentProcessing*)
6	PAYABLES	666	3	Maintain a fictitious vendor and enter a Vendor invoice for automatic payment (06-05)	(*APCreateOneTimeVendor* or *APVendorSetup*)	(*APBasicInvoiceProcessing* or *APBasicInvoiceProcessing* or *APInterfaceExpenseInvoices* or *APInterfaceExpenseInvoices* or *CBBasicProcessing* or *CBBasicProcessing* or *EDISetupAdmin* or *EDISetupAdmin* or *LMBasicProcessing* or
7	PAYABLES	667	3	Maintain a fictitious vendor and create a payment to that vendor	(*APCreateOneTimeVendor* or *APVendorSetup*)	(*APPaymentProcessing*)
8	PAYABLES	668	3	Enter fictitious vendor invoices and then render payment to the vendor (05-02)	(*APBasicInvoiceProcessing* or *APBasicInvoiceProcessing* or *APInterfaceExpenseInvoices* or *APInterfaceExpenseInvoices* or *CBBasicProcessing* or	(*APPaymentProcessing*)
9	PAYABLES	669	3	Purchase unauthorized items and initiate payment by invoicing (16-05)	(*POBasicPurchaseOrderProcessing* or *SSProcessEvent*)	(*APBasicInvoiceProcessing* or *APBasicInvoiceProcessing* or *APInterfaceExpenseInvoices* or *APInterfaceExpenseInvoices* or *CBBasicProcessing* or *CBBasicProcessing* or *EDISetupAdmin* or *EDISetupAdmin* or *LMBasicProcessing* or
10	PAYABLES	670	3	Enter fictitious vendor invoices and accept the goods via goods receipt (05-18)	(*APBasicInvoiceProcessing* or *APBasicInvoiceProcessing* or *APInterfaceExpenseInvoices* or *APInterfaceExpenseInvoices* or *CBBasicProcessing* or	(*APProcessingReportAccess* or *POInterfaceReceipts* or *POInterfaceReceipts* or *POProcessingReportAccess* or *POReceiving* or *POReceiving* or *RQReceiving* or *RQReceiving*)

The Policies and defining rules included in this report will be displayed.

Sheet 4: Function Code/ Actions Legend



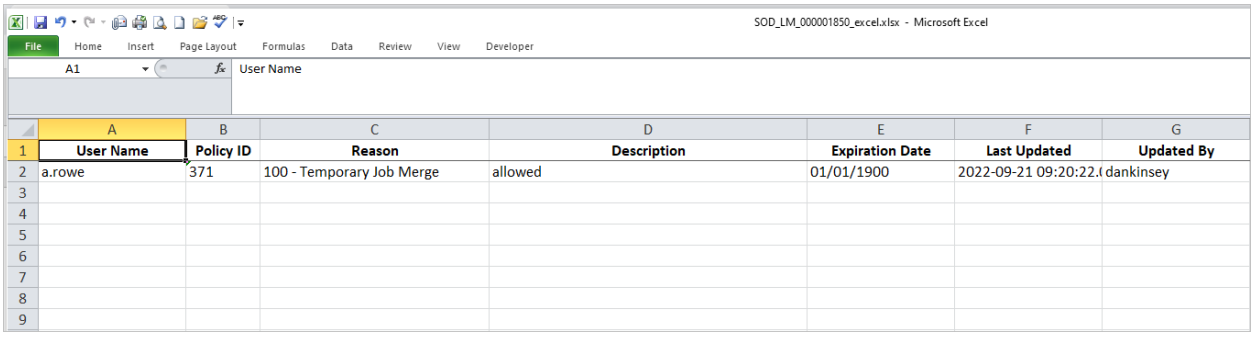
SOD_LS_000000069_excel.xlsx - Microsoft Excel

A1: Form/Function Code

Form/Function Code	+	-	A	C	D	F	I	N	P	R	S	T	V	X
HR11.1	PageDown	PageUp	Add	Change	Delete	FillDefaults	Inquire	Next	Previous	ReqDeductCreate				
PA13.2			Add	Change	Delete	FillDefaults	Inquire	Next	Previous					
PA31.1			Add	Change			Inquire	Next	Previous					
PR135			Add	Change	Delete		Inquire	Next	Previous	Reports	Submit		Validate Request	
PR137			Add	Change	Delete		Inquire	Next	Previous	Reports	Submit		Validate Request	
PR140			Add	Change	Delete		Inquire	Next	Previous	Reports	Submit		Validate Request	
PR160			Add	Change	Delete		Inquire	Next	Previous	Reports	Submit		Validate Request	
PR30.1	PageDown	PageUp	Add	Change			Inquire	Next	Previous					
PR35.1	PageDown	PageUp	Add	Change			Inquire	Next	Previous	Release		Totals		
PR35.2	PageDown	PageUp	Add	Change			Inquire	Next	Previous	Release		Totals		
PR35.3			Add									Totals		
PR35.4			Add									Totals		
PR35.5			Add									Totals		
PR35.6			Add									Totals		
PR35.8			Add									Totals		
PR36.1	PageDown	PageUp	Add	Change			Inquire	Next	Previous			Totals		Comments
PR37.1	PageDown	PageUp	Add	Change			Inquire			Release				

This sheet provides an explaination of what action or function code can be performed on a specific business class or token included in this report.

Sheet 5: Existing SoD Mitigations



SOD_LM_000001850_excel.xlsx - Microsoft Excel

A1: User Name

User Name	Policy ID	Reason	Description	Expiration Date	Last Updated	Updated By
a.rowe	371	100 - Temporary Job Merge	allowed	01/01/1900	2022-09-21 09:20:22.(	dankinsey

This will be a complete list of all User-Policy mitigations for violation shown on this report.

Note: This isn't necessarily all User-Policy mitigations. To get a complete list use the Mitigation Export option under SOD Mitigation on the Admin panel.

Sheet 6 – Mitigation Codes

Mitigation code	Description
100	Job Merge
200	Temporary Leave
250	Staff Shortage
300	Audit Approved
400	Access Approved
500	Allowable Action
600	Code 600
AA	Audit Approved

All available mitigation codes are displayed on this sheet.

Creating Mitigation using the Excel Upload

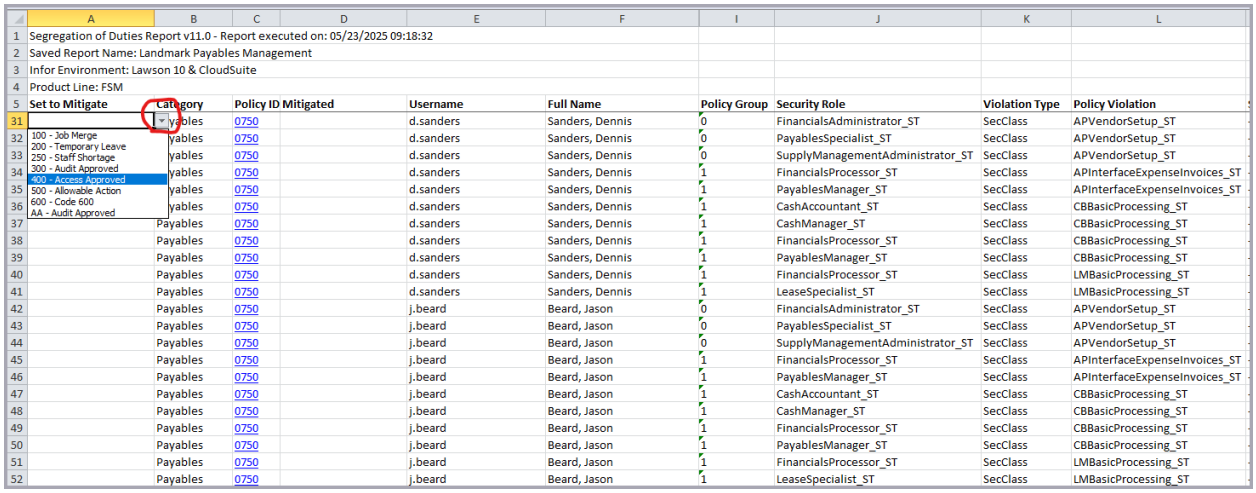
The Excel upload makes it easier to do mass mitigation updates. This option will allow you to create new mitigation reasons when needed and to assign mitigations to any user violation.

There are 3 options when working with Mitigations:

- Assign a new migitigation
- Change an existing mitigation reason
- Remove and existing mitigation

Assign or chancing a mitigation

Assigning a new mitigation simply requies you to select a mitigation code from the dropdown option in column A and drag it down on every line association with the user/policy combination. Activating the change requires an upload and import.



	A	B	C	D	E	F	I	J	K	L
1	Segregation of Duties Report v11.0 - Report executed on: 05/23/2025 09:18:32									
2	Saved Report Name: Landmark Payables Management									
3	Infor Environment: Lawson 10 & CloudSuite									
4	Product Line: FSM									
5	**Set to Mitigate**	**Category**	**Policy ID Mitigated**		**Username**	**Full Name**	**Policy Group**	**Security Role**	**Violation Type**	**Policy Violation**
31		yables	0750		d.sanders	Sanders, Dennis	0	FinancialsAdministrator_ST	SecClass	APVendorSetup_ST
32		yables	0750		d.sanders	Sanders, Dennis	0	PayablesSpecialist_ST	SecClass	APVendorSetup_ST
33		yables	0750		d.sanders	Sanders, Dennis	0	SupplyManagementAdministrator_ST	SecClass	APVendorSetup_ST
34		yables	0750		d.sanders	Sanders, Dennis	1	FinancialsProcessor_ST	SecClass	APInterfaceExpenseInvoices_ST
35		yables	0750		d.sanders	Sanders, Dennis	1	PayablesManager_ST	SecClass	APInterfaceExpenseInvoices_ST
36		yables	0750		d.sanders	Sanders, Dennis	1	CashAccountant_ST	SecClass	CBBasicProcessing_ST
37		Payables	0750		d.sanders	Sanders, Dennis	1	CashManager_ST	SecClass	CBBasicProcessing_ST
38		Payables	0750		d.sanders	Sanders, Dennis	1	FinancialsProcessor_ST	SecClass	CBBasicProcessing_ST
39		Payables	0750		d.sanders	Sanders, Dennis	1	PayablesManager_ST	SecClass	CBBasicProcessing_ST
40		Payables	0750		d.sanders	Sanders, Dennis	1	FinancialsProcessor_ST	SecClass	LMBasicProcessing_ST
41		Payables	0750		d.sanders	Sanders, Dennis	1	LeaseSpecialist_ST	SecClass	LMBasicProcessing_ST
42		Payables	0750		j.beard	Beard, Jason	0	FinancialsAdministrator_ST	SecClass	APVendorSetup_ST
43		Payables	0750		j.beard	Beard, Jason	0	PayablesSpecialist_ST	SecClass	APVendorSetup_ST
44		Payables	0750		j.beard	Beard, Jason	0	SupplyManagementAdministrator_ST	SecClass	APVendorSetup_ST
45		Payables	0750		j.beard	Beard, Jason	1	FinancialsProcessor_ST	SecClass	APInterfaceExpenseInvoices_ST
46		Payables	0750		j.beard	Beard, Jason	1	PayablesManager_ST	SecClass	APInterfaceExpenseInvoices_ST
47		Payables	0750		j.beard	Beard, Jason	1	CashAccountant_ST	SecClass	CBBasicProcessing_ST
48		Payables	0750		j.beard	Beard, Jason	1	CashManager_ST	SecClass	CBBasicProcessing_ST
49		Payables	0750		j.beard	Beard, Jason	1	FinancialsProcessor_ST	SecClass	CBBasicProcessing_ST
50		Payables	0750		j.beard	Beard, Jason	1	PayablesManager_ST	SecClass	CBBasicProcessing_ST
51		Payables	0750		j.beard	Beard, Jason	1	FinancialsProcessor_ST	SecClass	LMBasicProcessing_ST
52		Payables	0750		j.beard	Beard, Jason	1	LeaseSpecialist_ST	SecClass	LMBasicProcessing_ST

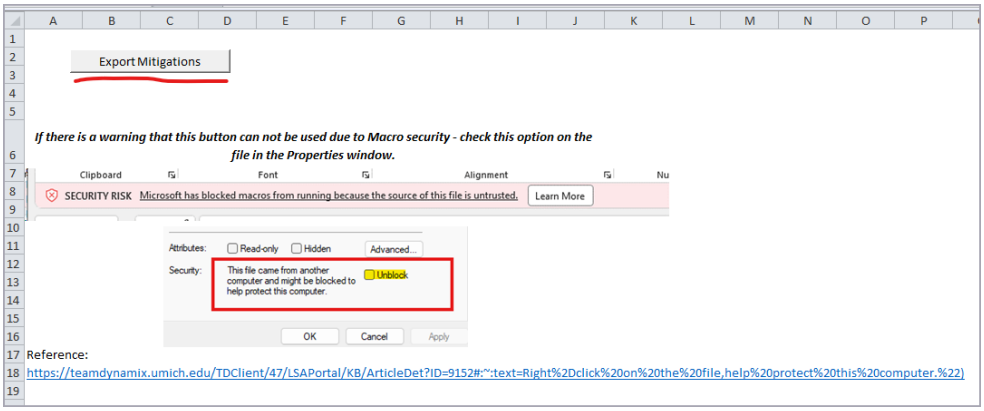
100 - Job Merge
200 - Temporary Leave
250 - Staff Shortage
300 - Audit Approved
400 - Access Approved
500 - Allowable Action
600 - Code 600
AA - Audit Approved

Deleting a mitigation

To delete an existing mitigation simply delete the value from the cell in column A for every row associated with the mitigation. Activating the deletion requires an upload and import.

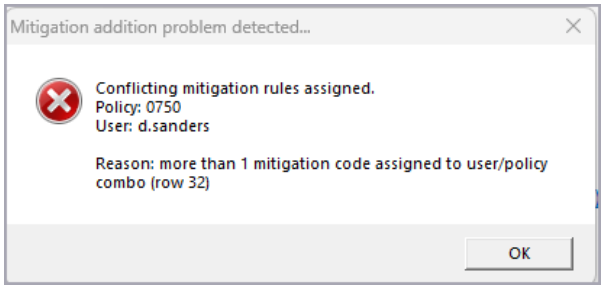
Creating the mitigation upload file.

The upload sheet provides an Export Mitigatons button. Selecting this will create and XML file that can be loaded through the Kinsey Admin panel.



Conflicting mitigation rules.

If you have more than 1 mitigation reason assigned to a user/policy violation or if you failed to drag the mitigation code onto every line associated with the violation you will receive an error message.

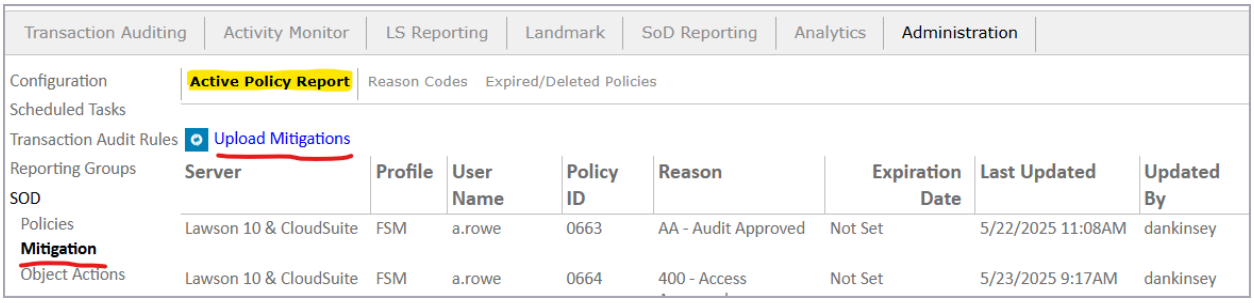


You can go back to the Violation sheet and make corrections prior to Exporting again.

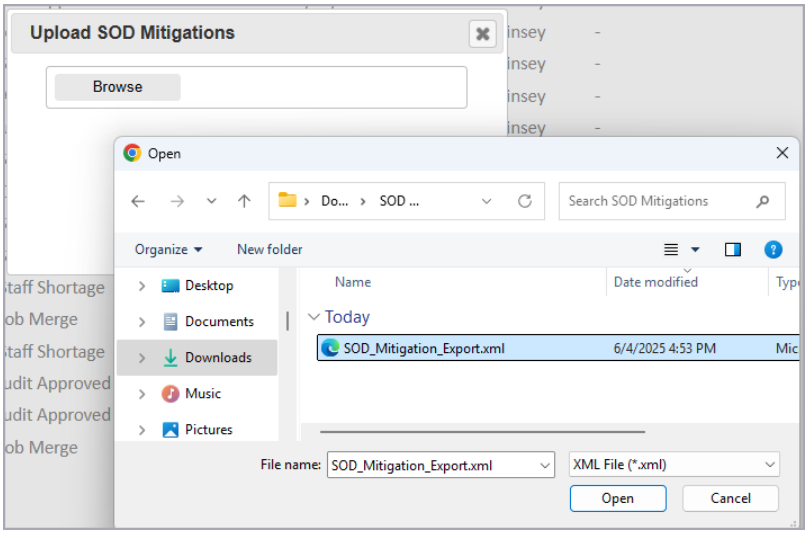
NOTICE: If a user is mitigated for ALL violations and you mitigated individual policies in Excel for the same user you will be notified that the new mitigations will not be active until you remove the All option in the Kinsey Admin panel under SOD mitigations.

Uploading the mitigation changes.

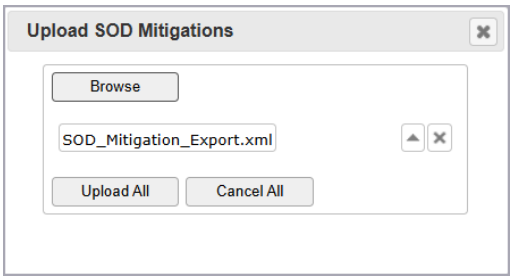
Log into the Kinsey portal and select Administration | SOD Mitigation | Active Policy Report tab



Select Upload Mitigations and browse to the location where you saved the export file.

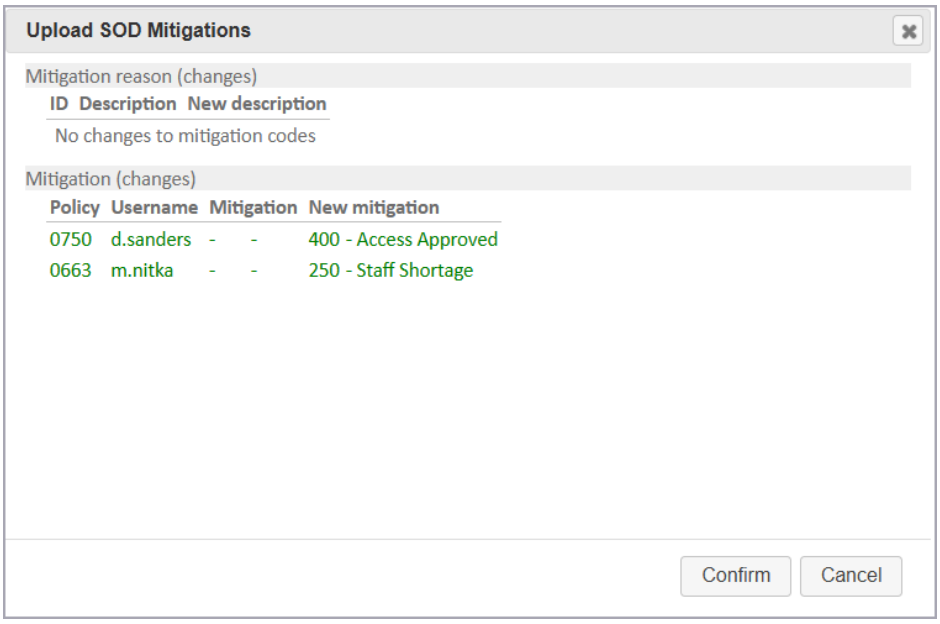


Select Upload All or Cancel All



The upload will give you an indication of the changes made. Items in green are new assignments, blue listing are changes and red and deletions.

At this point you still have the option of canceling the upload or confirming.



Backing our your changes.

One option if there is concern that mistake may be made is to save the Excel document with a new name prior to making your mitigation changes. If you feel that after you have assigned, uploaded and imported the mitigaitions that you want to start over you can simply use the backup excel document and create an upload XML file. When you import the file through the Kinsey portal the application will recognize the changes and reset your policies.

Notes: