kinsey™

Segregation of Duties User Guide

Document containing setup and reporting instructions related to Segregation of Duties

2016

0902A

Contents

Introduction

Kinsey's Segregation of Duties (SoD) Reporting is designed to examine LAUA Security Classes or LS Users to determine if there is a violation to an SoD policy. The delivered 240 policies cover applications included in all 3 Lawson suites. An unlimited number of new policies can be added or existing policies can be changed to align with your organization. The SoD report can be generated at any time by an authorized user and will identify the policy that has been violated and the specific assignments that have caused the violation.

Features:

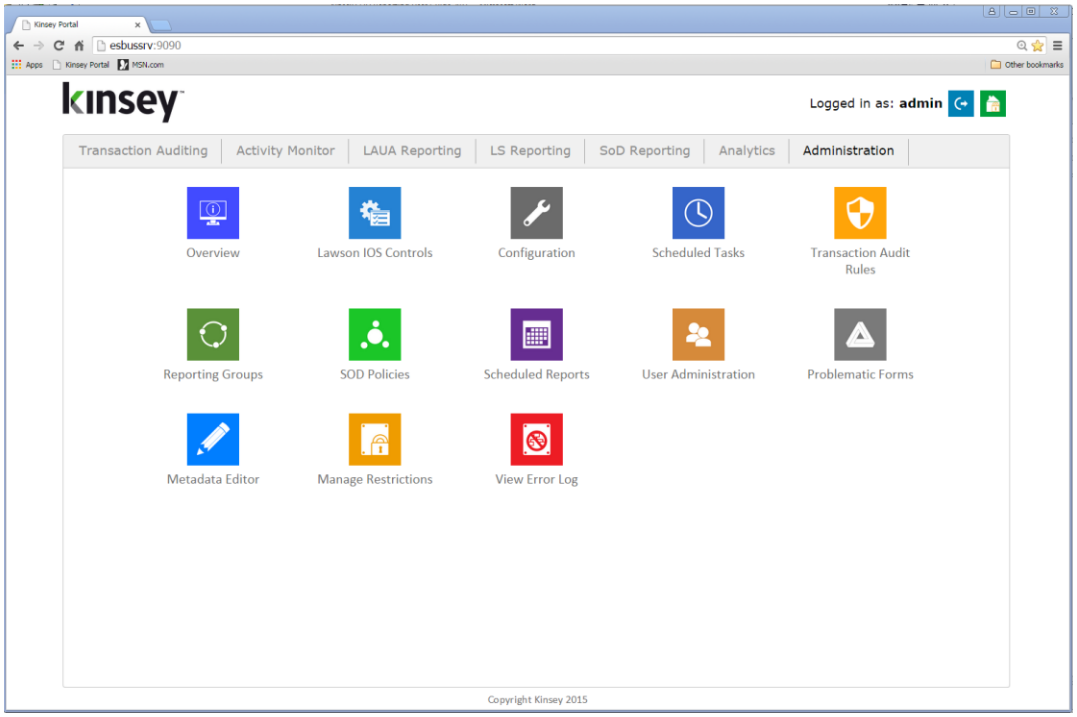
- Delivered with 240 prebuilt policies
- Ability to add an unlimited number of policies and rules
- Ability to activate and rank policies individually
- Uses nested And/Or logic to enhance the flexibility and granularity of the rules
- Predefined reports by User, by Policy or by User Role grouping
- Excel export
- Differences Reporting

Administration

Users

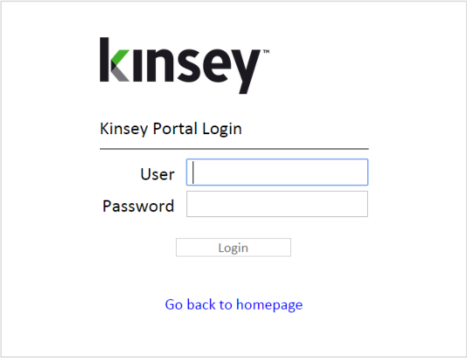
Initially you will need to identify the users who will have access to the SoD Reports and administrative functions.

Using the URL provided during the installation launch the Kinsey Portal home page.

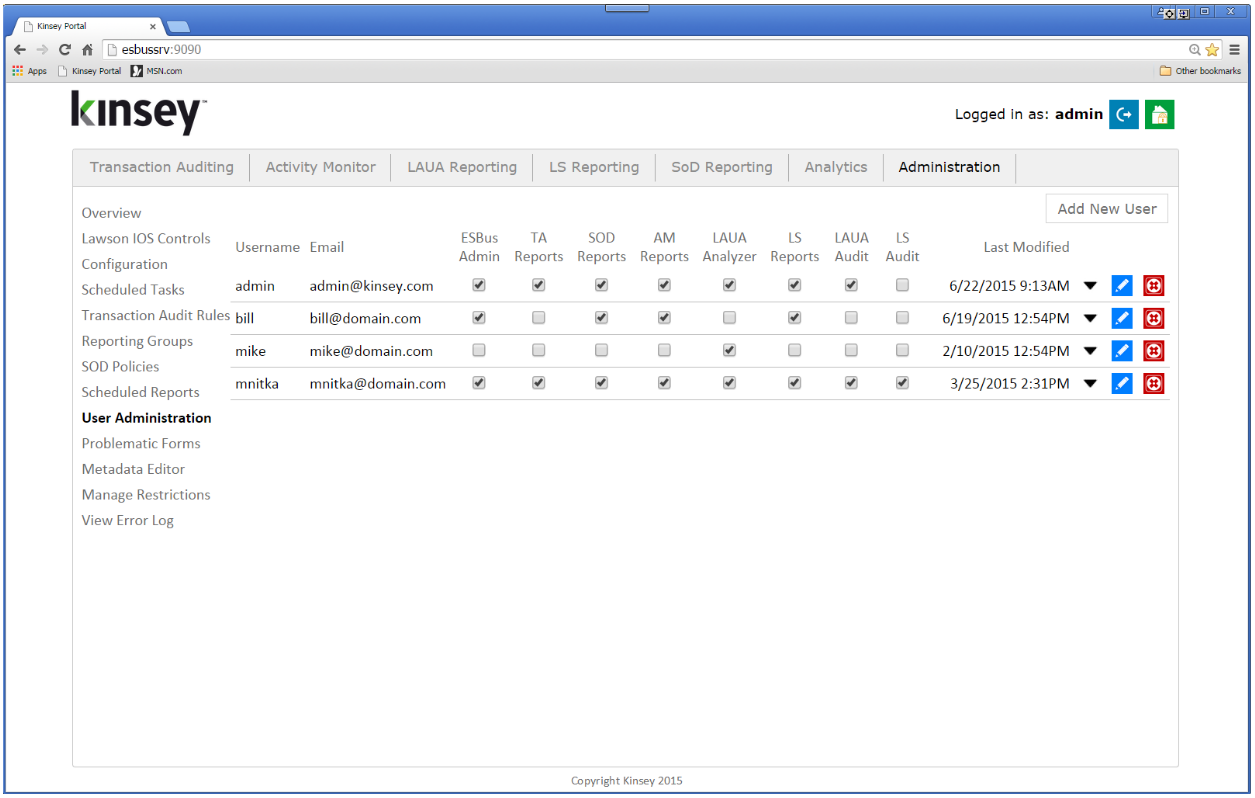


To add or change the user assignments select **User Administration** from the **Administration** Portal page.

If this is the first time you are accessing an applicationfrom the Kinsey portal you will need to login using the link in the top right corner of your screen. Once you have logged in you will have access to any application the system administrator has granted you access to.



Setting up a New User



Username	Email	ESBus Admin	TA Reports	SOD Reports	AM Reports	LAUA Analyzer	LS Reports	LAUA Audit	LS Audit	Last Modified
admin	admin@kinsey.com	☑	☑	☑	☑	☑	☑	☑	□	6/22/2015 9:13AM
bill	bill@domain.com	☑	□	☑	☑	□	☑	□	□	6/19/2015 12:54PM
mike	mike@domain.com	□	□	□	□	☑	□	□	□	2/10/2015 12:54PM
mnitka	mnitka@domain.com	☑	☑	☑	☑	☑	☑	☑	☑	3/25/2015 2:31PM

To add a user to the system select the Add New User button, complete the form and select the applications you would like the user to access.

For more information on setting up a new user please refer to the Kinsey Admin Guide.

Policy Maintenance

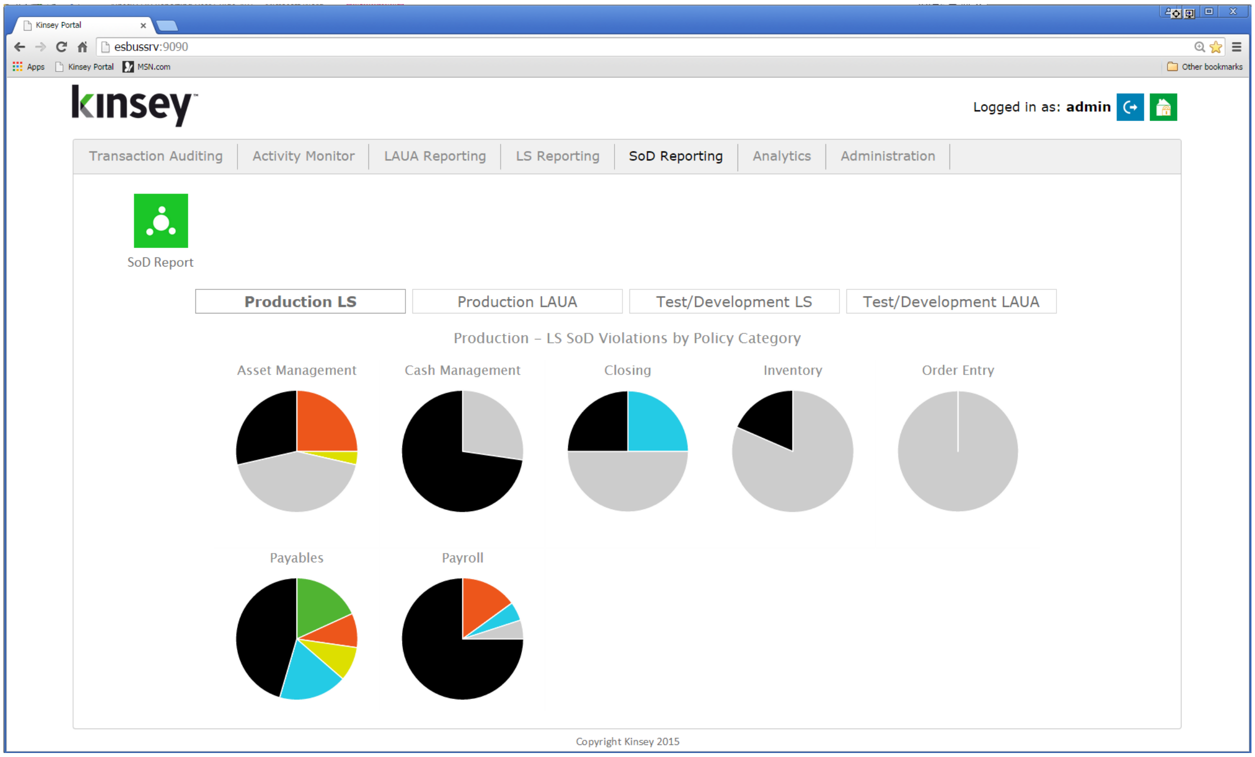
Refer to the SoD policy Maintenance section of the Kinsey Administor Guide for information on how to create and maintain SoD policies.

SOD Configuration

Refer to the SoD policy Coniguration section of the Kinsey Administor Guide for information on how to maintain the SoD Configuration.

Reporting

Using the URL provided during the installation launch the Kinsey Portal home page.

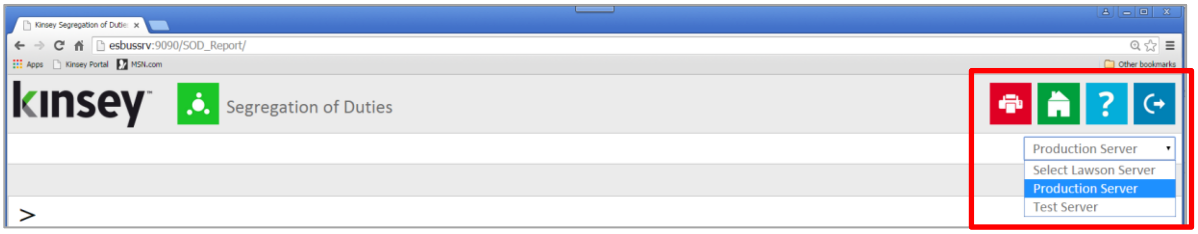


Select the *SOD Reporting* tab and log into the applicaiton. The dashboard will display a violation pie chart for each policy category. By default the application display's charts for the LS Production environment but thress other options are provide.

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

Black	Inactive policies
Grey	Policies that do not have any violations
Sky Blue	5 Star policies in violations
Yellow	4 Star policies in violation
Orange	3 Star policies in violation
Green	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.



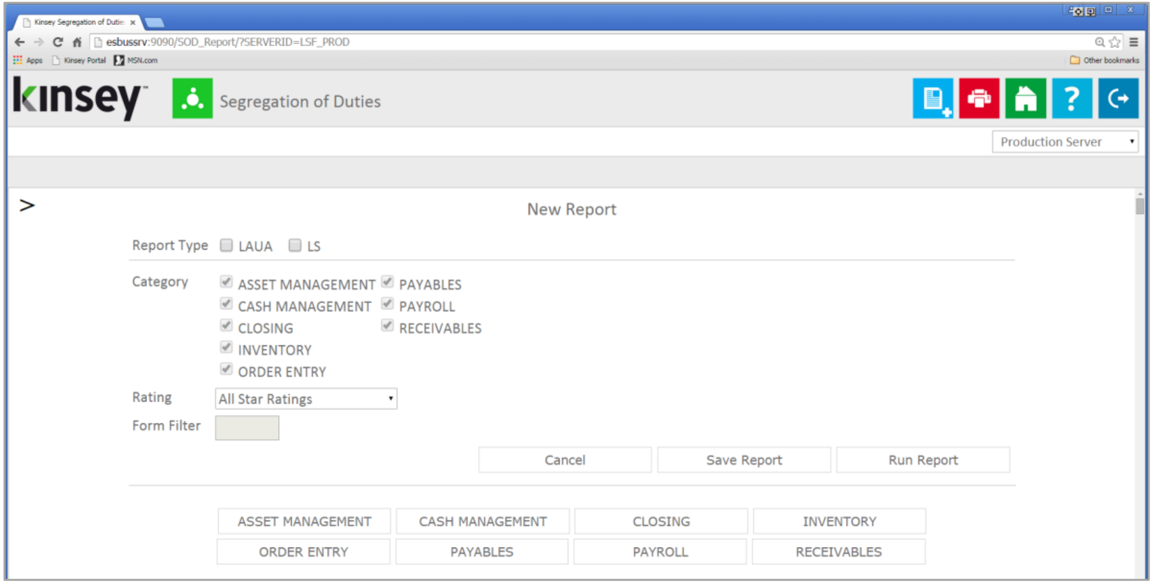
esbussrv:9090/SOD_Report/

Production Server

- Select Lawson Server
- Production Server
- Test Server

Creating a New Report

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



esbussrv:9090/SOD_Report/?SERVERID=LSF_PROD

Production Server

New Report

Report Type ☐ LAUA ☐ LS

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

Rating: All Star Ratings

Form Filter:

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 and/or LAUA check boxes for the security model you would like to validate.

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

- Security Class Violation Report – this report will report violations for each LS User or for each LAUA Security Class.
- Role Test Report – this report will report on violations for any Role or combination of Roles in LS. This is not an option for LAUA security.

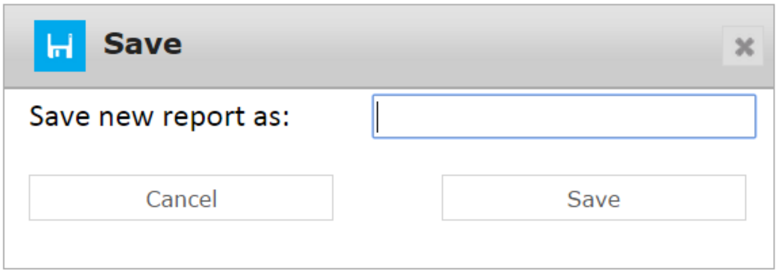
To create a SoD violation report use only the Category, Level of Importance and Form filters to make your selections.

Category: By default all categories are selected when you define a new report. Simply uncheck a category to omit 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" on page 8 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 'begins' with 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.

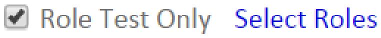


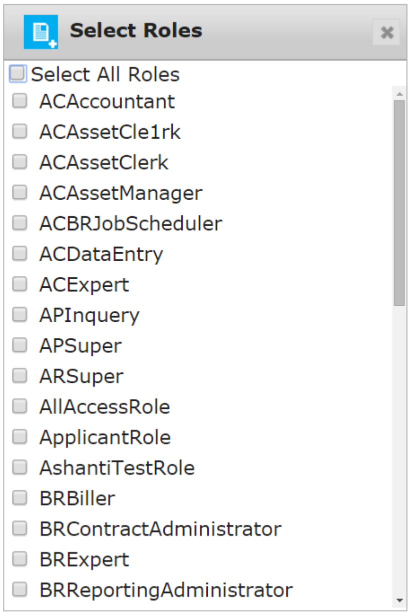
Note: the system does not store the Form filter or the Level of Importance with the report parameters, rather it stores the actual policies selected. If you edit an existing report you can revise your policy list by using the check box next to the policy number. See Editing a Report for more information

Creating a Role Test Report (Security 9/10 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 in LS.





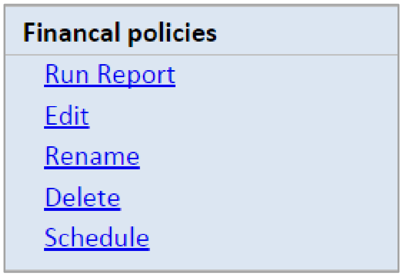
□ Select All Roles
□ ACAccountant
□ ACAssetCle1rk
□ ACAssetClerk
□ ACAssetManager
□ ACBRJobScheduler
□ ACDataEntry
□ ACExpert
□ APInquery
□ APSuper
□ ARSuper
□ AllAccessRole
□ ApplicantRole
□ AshantiTestRole
□ BRBiller
□ BRContractAdministrator
□ BRExpert
□ BRReportingAdministrator

When the list of roles is displayed you can choose any combination of roles you would like to test. When you are finished making your selection close the window to continue.

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, 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".

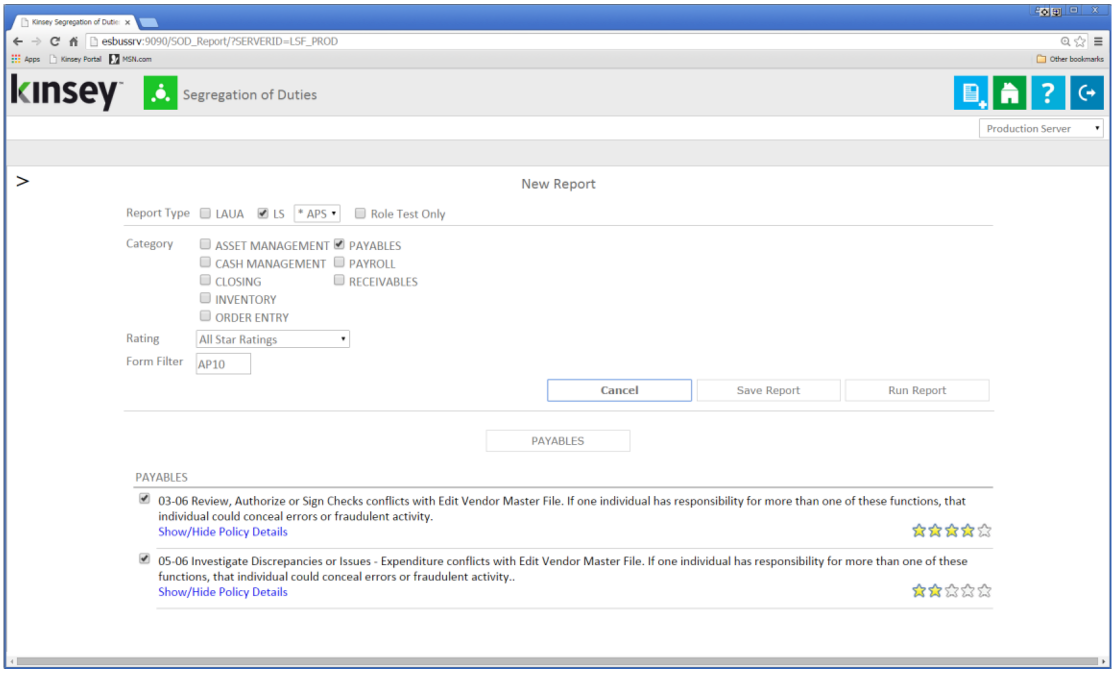


The edit option will display the same set of parameters as found with a new report. When a new report is saved only the Category selection and the list of policies are saved by the system. The Level of Importance and the Form Filter parameters are not saved.

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.

For example, let's create a report for all policies that include token AP10.1. To do this I would select Payables, All Star Ratings and enter a Form Filter of AP10.

This system will display 2 polices the meet this criteria.



New Report

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: AP10

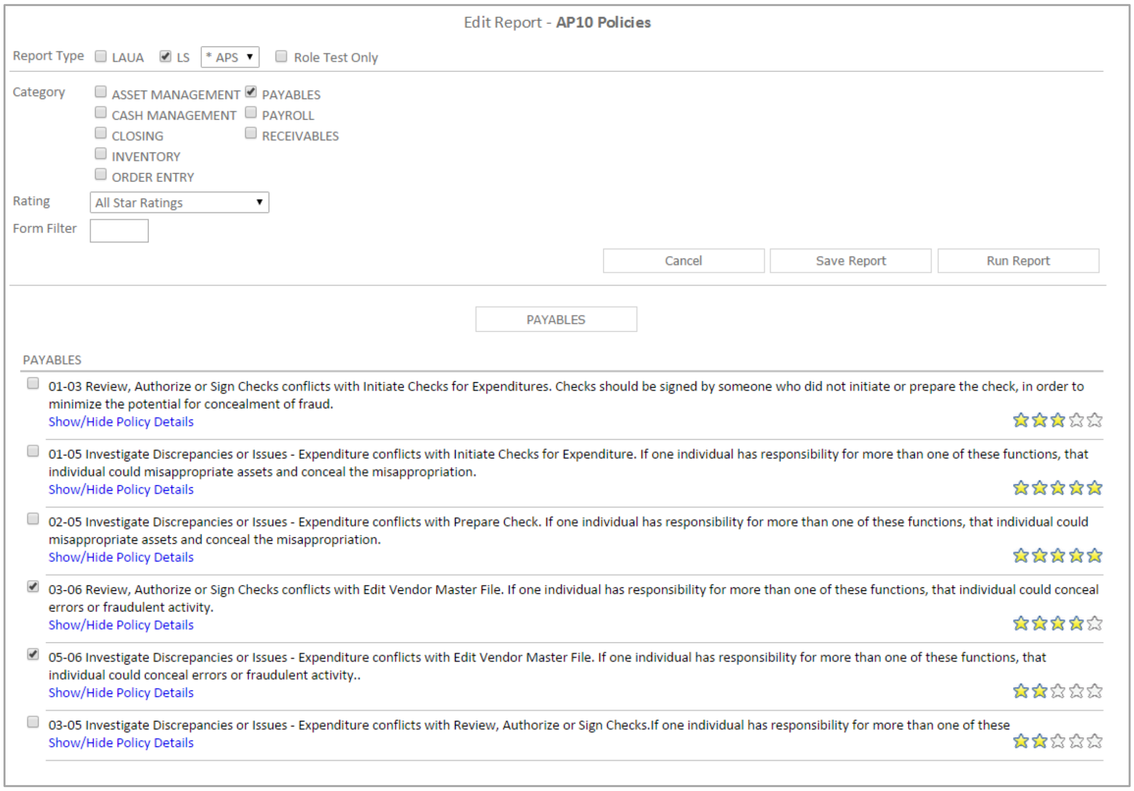
PAYABLES

☑ 03-06 Review, Authorize or Sign Checks conflicts with Edit Vendor Master File. If one individual has responsibility for more than one of these functions, that individual could conceal errors or fraudulent activity.
Show/Hide Policy Details ★★★★☆

☑ 05-06 Investigate Discrepancies or Issues - Expenditure conflicts with Edit Vendor Master File. If one individual has responsibility for more than one of these functions, that individual could conceal errors or fraudulent activity..
Show/Hide Policy Details ★★☆☆☆

When I save the report the application will store the selected Category and 2 policies but NOT the star rating or form filter.

When I edit the report the system will display all Payable policies available with the two that were previously saved.



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:

PAYABLES

☐ 01-03 Review, Authorize or Sign Checks conflicts with Initiate Checks for Expenditures. Checks should be signed by someone who did not initiate or prepare the check, in order to minimize the potential for concealment of fraud.
Show/Hide Policy Details ★★★☆☆

☐ 01-05 Investigate Discrepancies or Issues - Expenditure conflicts with Initiate Checks for Expenditure. 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 ★★★★★

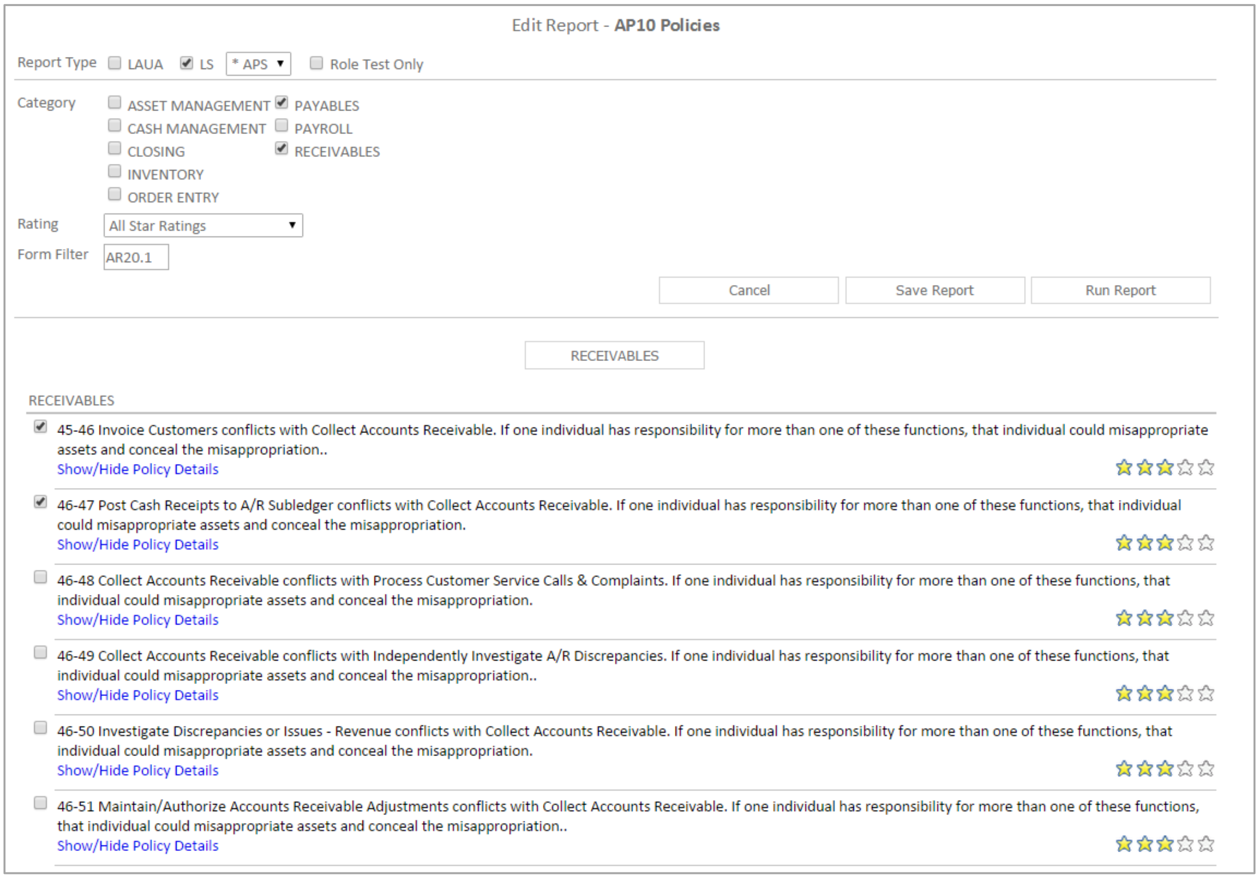
☐ 02-05 Investigate Discrepancies or Issues - Expenditure conflicts with Prepare Check. If one individual has responsibility for more than one of these functions, that individual could misappropriate assets and conceal the misappropriation.
Show/Hide Policy Details ★★★★★

☑ 03-06 Review, Authorize or Sign Checks conflicts with Edit Vendor Master File. If one individual has responsibility for more than one of these functions, that individual could conceal errors or fraudulent activity.
Show/Hide Policy Details ★★★★☆

☑ 05-06 Investigate Discrepancies or Issues - Expenditure conflicts with Edit Vendor Master File. If one individual has responsibility for more than one of these functions, that individual could conceal errors or fraudulent activity..
Show/Hide Policy Details ★★☆☆☆

☐ 03-05 Investigate Discrepancies or Issues - Expenditure conflicts with Review, Authorize or Sign Checks.If one individual has responsibility for more than one of these
Show/Hide Policy Details ★★☆☆☆

I can now select additional Payable policies, add a category, change the rating or enter a form filter. However if I want to add all policies containing AR20.1 I need to check the *RECEIVABLES* category and enter AR20.1 in the form filter then manually check policies I want to add. See example below.



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 ★★★☆☆

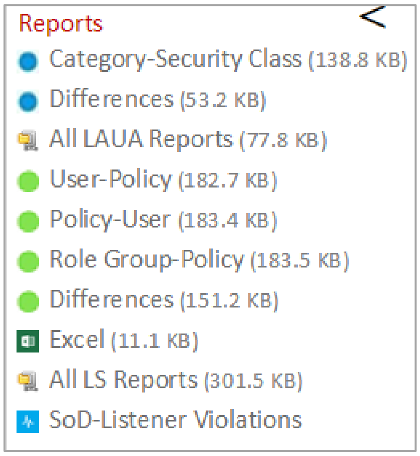
At this point if I select SAVE REPORT ***I will only be saving what is displayed on the screen.*** If I want the report to include the Payable policies previously saved I need to clear the Form Filter field. The application will display a complete list of Payable and Receivable polices with only the required policies checked.

Running a Report

To run a saved report simply click on the report name and select Run Report. The application will include one LAUA format and 5 Security 9/10 formats. You can immediately view the report in your browser or save the file to be viewed at a later time.

The zipped report contains the HTML file, which can be downloaded and saved or e-mailed to other employees.

LAUA Reports are maked with a blue dot, LS reports with a green dot.



Reports

- Category-Security Class (138.8 KB)
- Differences (53.2 KB)
- All LAUA Reports (77.8 KB)
- User-Policy (182.7 KB)
- Policy-User (183.4 KB)
- Role Group-Policy (183.5 KB)
- Differences (151.2 KB)
- Excel (11.1 KB)
- All LS Reports (301.5 KB)
- SoD-Listener Violations

LAUA Report

The LAUA Report provides a list of violations sorted by Policy then Security Class.

LAUA Differences Report

The difference report will show you any changes made to the report since the last time it was run.

LS Report-Sorted by User

This version of the report will provide a list of violated policies sorted by User then Policy. This returns a list of all policies violated by a user.

LS9 Report-Sorted by Rule

This version of the report will provide a list of violated policies sorted by Policy then User. This returns a list of all users that violate a policy.

LS9 Report-Sorted by Role Group

This version of the report group's users together based on their assigned security roles. By doing this you can see if a group of users with the same assigned roles are violating any particular policy. This will allow you to resolve a policy violation for 1 user and all of the users assigned the same roles will also be resolved.

LS9 Differences Report

The difference report will show you any changes made to the report since the last time it 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

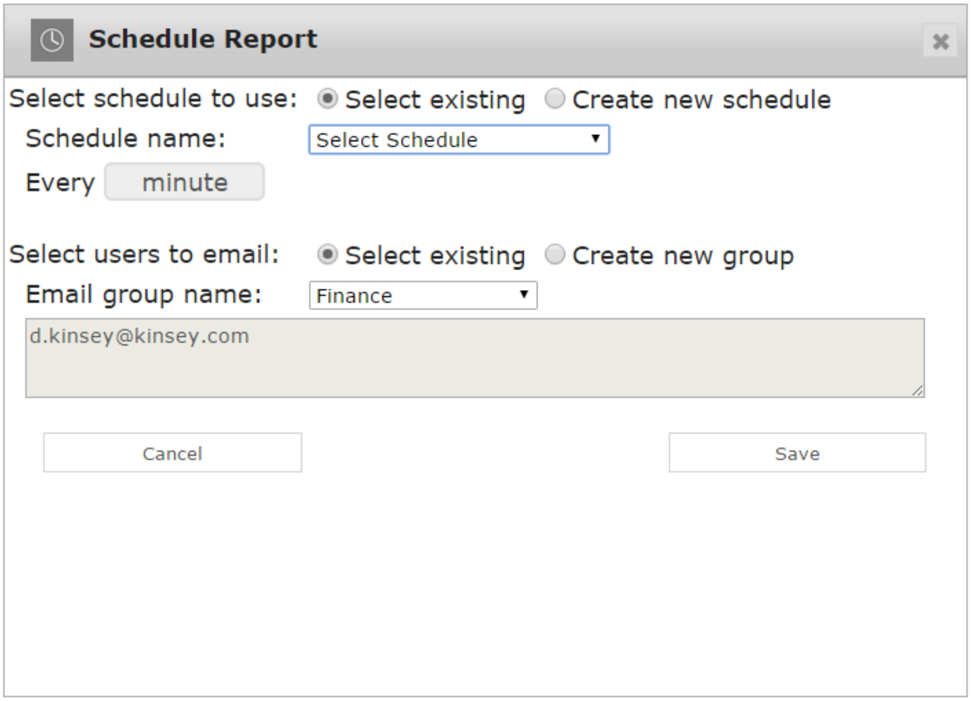
To rename an existing report click on the report name and select *Delete*.

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 if a schedule exists for a report but it is not enabled. A blue clock indicates that the schedule is currently enabled and running.



Schedule Report

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

Schedule name: Select Schedule

Every minute

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

Email group name: Finance

d.kinsey@kinsey.com

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. Select the appropriate option and follow the on screen prompts.

You can also create or use existing reporting groups. A reporting group contains a list of users you want to receive the report. Enter the appropriate email address for each user.

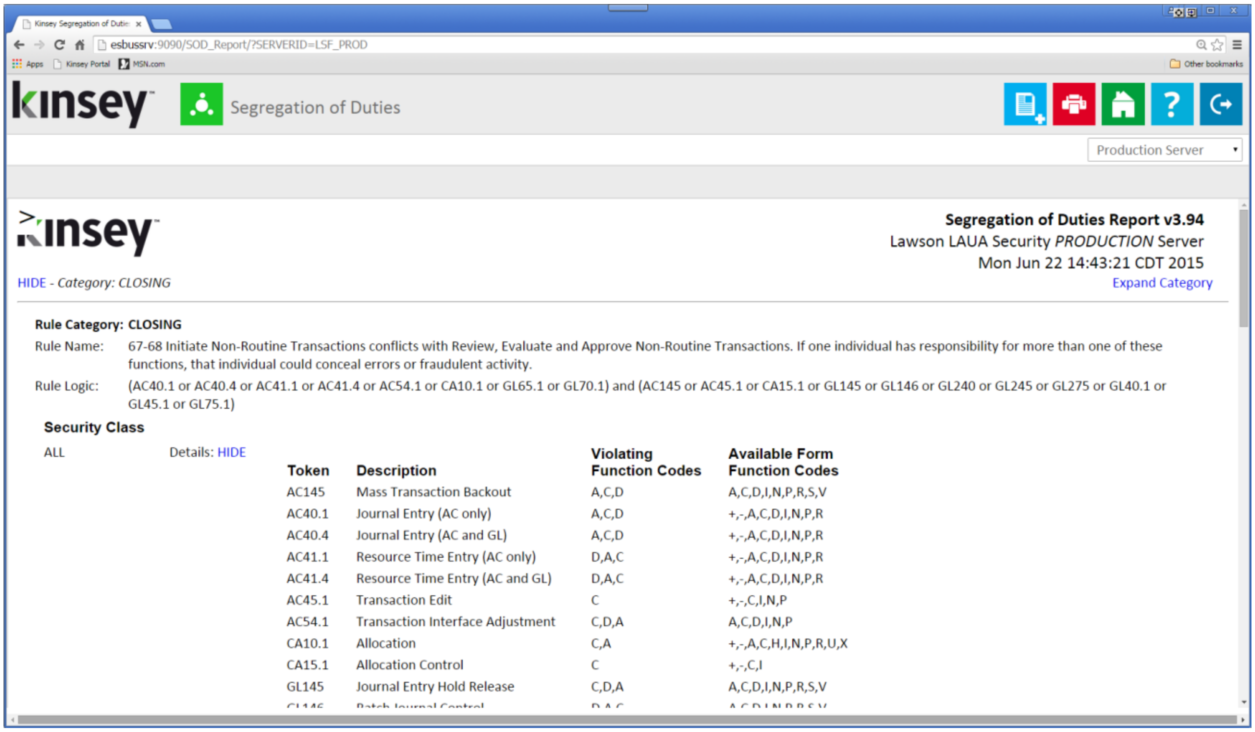
Activating or Deactivating a Scheduled Report

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.

LAUA Report – *By Security Class*



Segregation of Duties Report v3.94
Lawson LAUA Security *PRODUCTION* Server
Mon Jun 22 14:43:21 CDT 2015

HIDE - *Category: CLOSING*

Expand Category

Rule Category: CLOSING

Rule Name: 67-68 Initiate Non-Routine Transactions conflicts with Review, Evaluate and Approve Non-Routine Transactions. If one individual has responsibility for more than one of these functions, that individual could conceal errors or fraudulent activity.

Rule Logic: (AC40.1 or AC40.4 or AC41.1 or AC41.4 or AC54.1 or CA10.1 or GL65.1 or GL70.1) and (AC145 or AC45.1 or CA15.1 or GL145 or GL146 or GL240 or GL245 or GL275 or GL40.1 or GL45.1 or GL75.1)

Security Class

ALL Details: HIDE

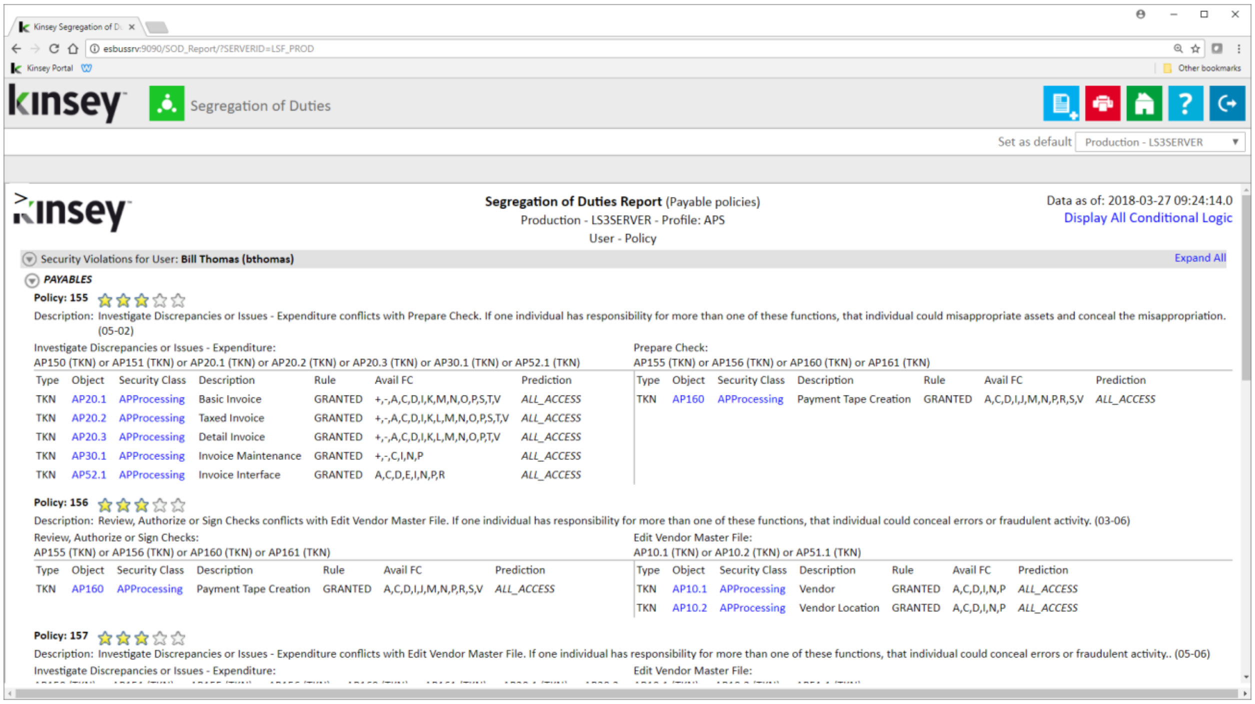
Token	Description	Violating Function Codes	Available Form Function Codes
AC145	Mass Transaction Backout	A,C,D	A,C,D,I,N,P,R,S,V
AC40.1	Journal Entry (AC only)	A,C,D	+,-,A,C,D,I,N,P,R
AC40.4	Journal Entry (AC and GL)	A,C,D	+,-,A,C,D,I,N,P,R
AC41.1	Resource Time Entry (AC only)	D,A,C	+,-,A,C,D,I,N,P,R
AC41.4	Resource Time Entry (AC and GL)	D,A,C	+,-,A,C,D,I,N,P,R
AC45.1	Transaction Edit	C	+,-,C,I,N,P
AC54.1	Transaction Interface Adjustment	C,D,A	A,C,D,I,N,P
CA10.1	Allocation	C,A	+,-,A,C,H,I,N,P,R,U,X
CA15.1	Allocation Control	C	+,-,C,I
GL145	Journal Entry Hold Release	C,D,A	A,C,D,I,N,P,R,S,V
GL146	Batch Journal Control	D,A,C	A,C,D,I,N,P,R,S,V

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

LAUA Report – Differences

The differences report will show any changes to the report since the last time it was run.

LS Report - *By User/Policy*



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

Data as of: 2018-03-27 09:24:14.0

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

PAYABLES

Policy: 155 ★★★☆☆

Description: Investigate Discrepancies or Issues - Expenditure conflicts with Prepare Check. If one individual has responsibility for more than one of these functions, that individual could misappropriate assets and conceal the misappropriation. (05-02)

Investigate Discrepancies or Issues - Expenditure:
AP150 (TKN) or AP151 (TKN) or AP20.1 (TKN) or AP20.2 (TKN) or AP20.3 (TKN) or AP30.1 (TKN) or AP52.1 (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*
TKN	AP20.2	APProcessing	Taxed Invoice	GRANTED	+,-,A,C,D,I,K,L,M,N,O,P,S,T,V	*ALL_ACCESS*
TKN	AP20.3	APProcessing	Detail Invoice	GRANTED	+,-,A,C,D,I,K,L,M,N,O,P,T,V	*ALL_ACCESS*
TKN	AP30.1	APProcessing	Invoice Maintenance	GRANTED	+,-,C,I,N,P	*ALL_ACCESS*
TKN	AP52.1	APProcessing	Invoice Interface	GRANTED	A,C,D,E,I,N,P,R	*ALL_ACCESS*

Prepare Check:
AP155 (TKN) or AP156 (TKN) or AP160 (TKN) or AP161 (TKN)

Type	Object	Security Class	Description	Rule	Avail FC	Prediction
TKN	AP160	APProcessing	Payment Tape Creation	GRANTED	A,C,D,I,J,M,N,P,R,S,V	*ALL_ACCESS*

Policy: 156 ★★★☆☆

Description: Review, Authorize or Sign Checks conflicts with Edit Vendor Master File. If one individual has responsibility for more than one of these functions, that individual could conceal errors or fraudulent activity. (03-06)

Review, Authorize or Sign Checks:
AP155 (TKN) or AP156 (TKN) or AP160 (TKN) or AP161 (TKN)

Type	Object	Security Class	Description	Rule	Avail FC	Prediction
TKN	AP160	APProcessing	Payment Tape Creation	GRANTED	A,C,D,I,J,M,N,P,R,S,V	*ALL_ACCESS*

Edit Vendor Master File:
AP10.1 (TKN) or AP10.2 (TKN) or AP51.1 (TKN)

Type	Object	Security Class	Description	Rule	Avail FC	Prediction
TKN	AP10.1	APProcessing	Vendor	GRANTED	A,C,D,I,N,P	*ALL_ACCESS*
TKN	AP10.2	APProcessing	Vendor Location	GRANTED	A,C,D,I,N,P	*ALL_ACCESS*

Policy: 157 ★★★☆☆

Description: Investigate Discrepancies or Issues - Expenditure conflicts with Edit Vendor Master File. If one individual has responsibility for more than one of these functions, that individual could conceal errors or fraudulent activity.. (05-06)

Investigate Discrepancies or Issues - Expenditure:

Edit Vendor Master File:

The User report shows all violations for each Lawson User.

LS Report – *By Policy/User*

The Policy/User report will displays the same information as the User/Polciy report but the information is sorted by Policy.

LS Report – *By Policy/User*

The Policy/User report displays the same information as the User/Polciy report but the information is sorted by Policy.

LS Report – *By Role Group/Policy*

The Role Group/User report displays the same information as the User/Polciy report but the information is sorted based a Role Group created during the report. A Role Group is created on demand for all users that share the same Role assigments.

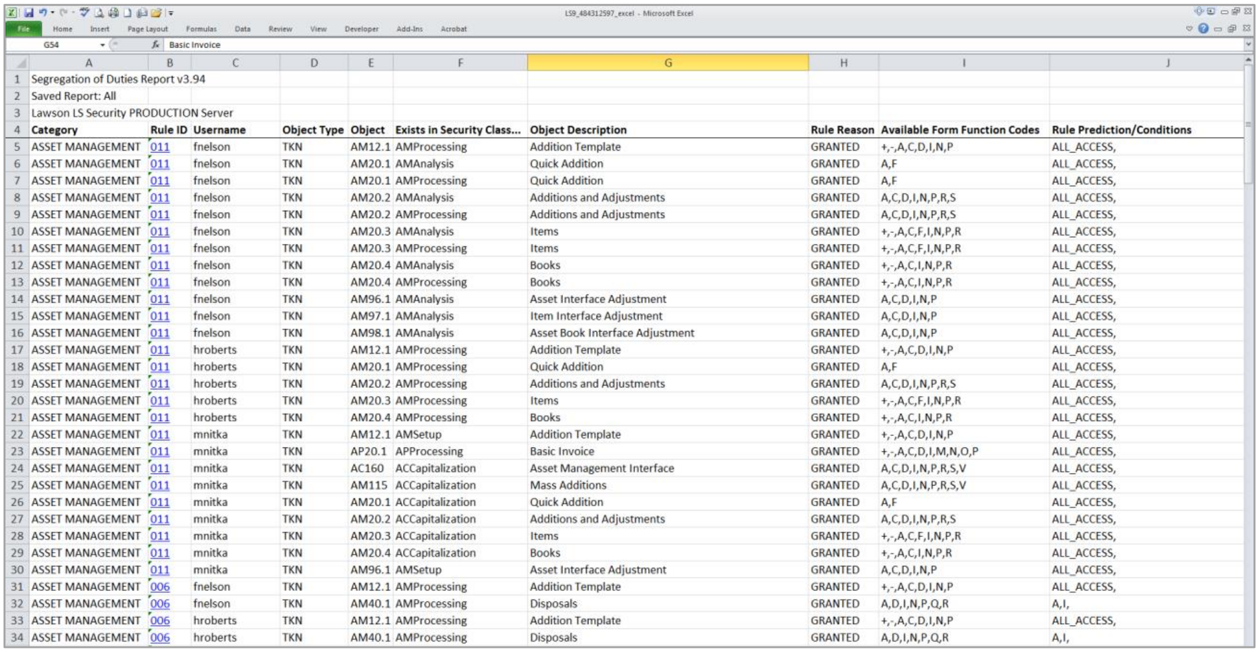
LS Report – *Differences*

The differences report will show any changes to the report since the last time it was run.

LS Report – *Excel*

The Export version of the report creates 4 separate sheets. The first sheet consist 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 a easy way to evaluate the number of over all violations you have in your security model. The third sheet provide a list of the policies included in the report and the fourth sheet provide a legend of the Function Codes used in the report.

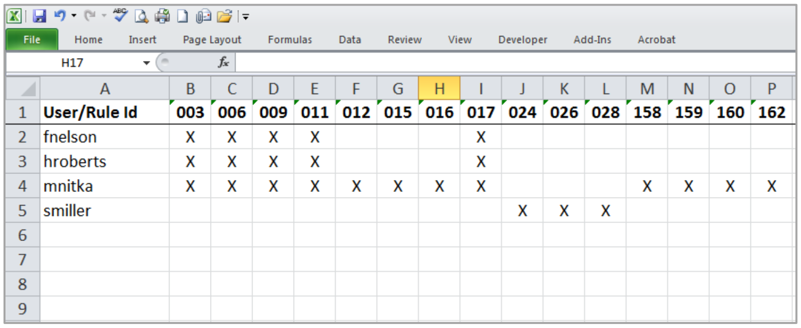
Excel Violation Report



G54 Basic Invoice

	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



H17

	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							
4	mnitka	X	X	X	X	X	X	X	X				X	X	X	X
5	smiller									X	X	X				
6																
7																
8																
9																

Notes: