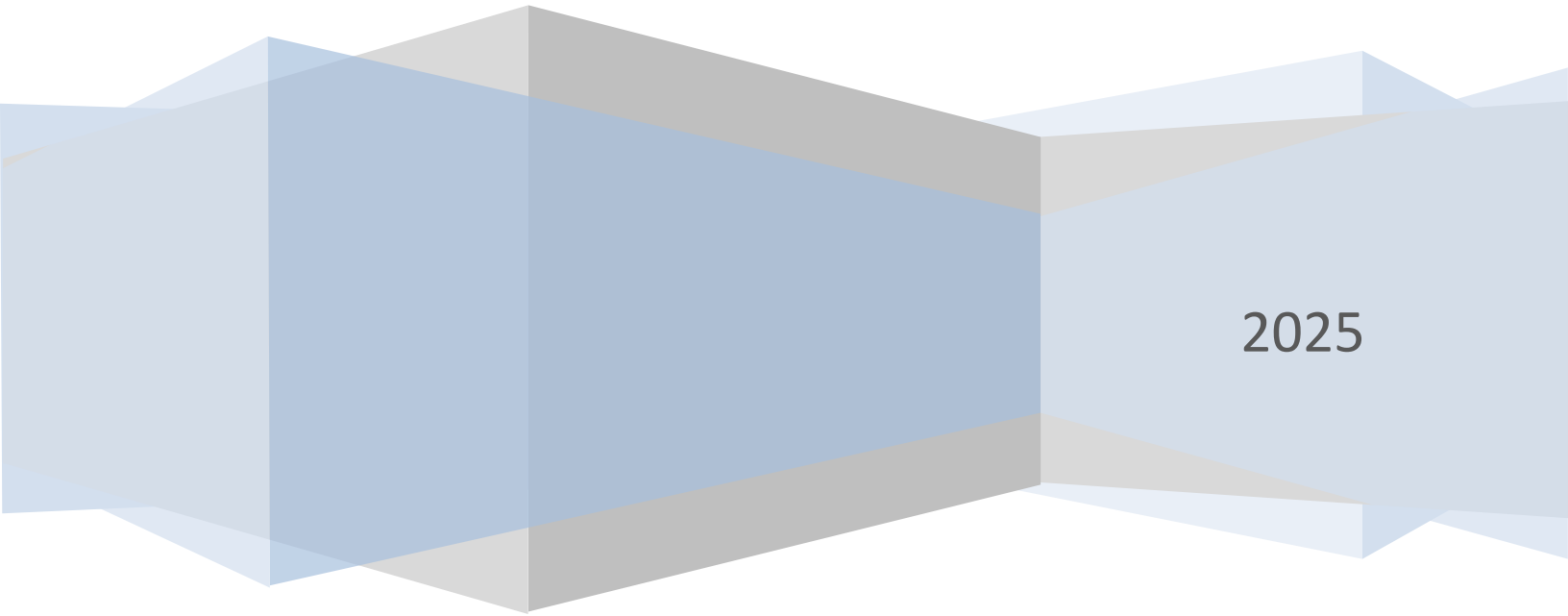
Administrator Guide

Document contains administration instructions related to Transaction Auditing, Activity Monitor, Segregation of Duties, Security Reporting and Security Auditing for both Lawson S3 and (CloudSuite) Landmark



2025

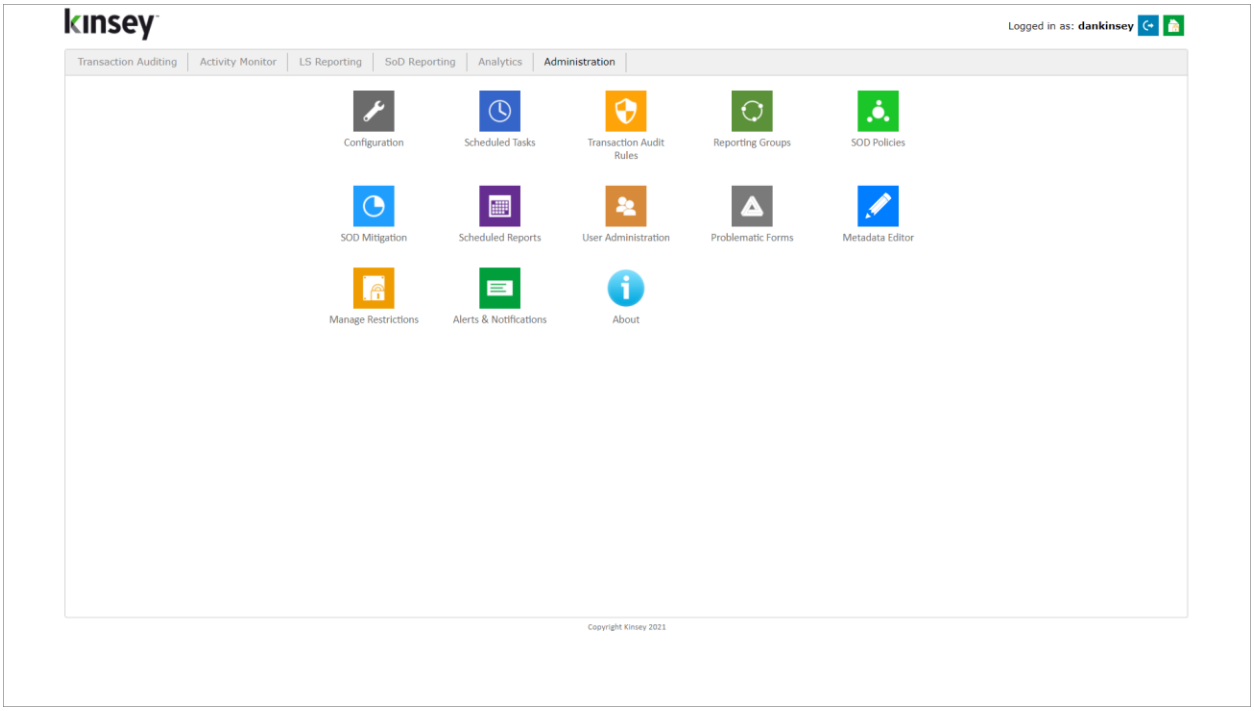
Table of Contents

Administrative Login 4
Configuration 5
Basic Server Configuration 5
Global Configuration 5
Transaction Auditing Global Configuration 5
Segregation of Duties Global (SoD) Configuration (S3 only) 6
Temporary File Locations 7
Infor ADFS Configurtation (Production Server) 7
Lawson Configuration Production Server 7
LS Security Configuration (Production Server) 8
Landmark Configuration (Prod) 8
Infor ADFS Configuration (Test Server) 9
Lawson Configuration (Test Server) 9
LS Security Configuration (TEST Server) 9
Scheduled Tasks 9
On Demand Tasks 9
Defining a Schedule 10
Transaction Audit Rules 11
Creating or Changing an Audit Rule for Lawson S3 12
Creating, Changing or Deleting an Audit Rule for CloudSuite (Landmark) 13
Reporting Groups 15
Assigning or Removing a User to a Group 15
SOD Policy Maintenance 17
Auditing a Policy (S3 only) 18
Enabling/Disabling a Policy 18
Rating a Policy's Level of Importance 18
Viewing or Editing a Policy 19
Adding an Object to an existing policy (S3) 20
Adding an Object to an existing policy (Landmark) 21
Deleting an Object from an existing policy 21

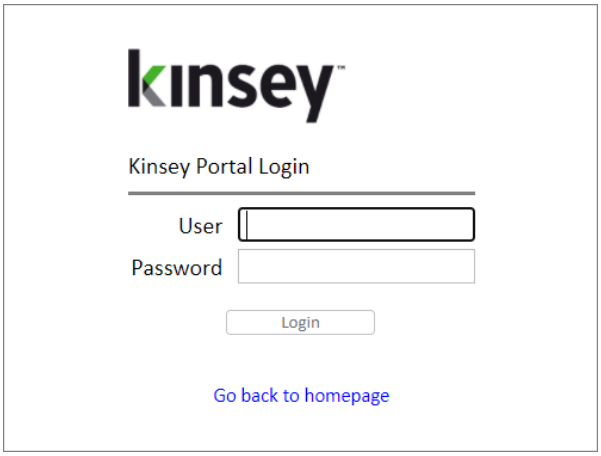
Adding a Group to an existing policy 21
Deleting a Group from an existing policy 21
Creating a New Policy 21
Deleting a Policy 22
SOD Mitigation 22
Active Policies Report 23
Reason Codes 23
Expired/Deleted Policies 24
SOD Object Actions (Landmark) 25
SOD Configuration 26
Lawson V10 (S3) 26
Scheduled Reports 28
Enabling or Disabling a Scheduled Report 28
Editing Schedules 30
Report Snapshots 31
User Administration 32
Detailed Application Security Settings 32
Report Restrictions (Transaction Audit Reports) 33
Changing or Deleting a User 35
Alerts and Notifications 36
Commonly Asked Questions 37
Administrative 37
Segregation of Duties 38
LS Reporting 38
Activity Monitor (Listener) 39
Problem Resolution 40
Virtual Server System Settings 40
Potential Lawson Issues 41
Virtual Server Monitoring 42
LS Reporting Data Collection Problems 43

Administrative Login

You'll have your own custom URL for accessing the Kinsey Server's main menu.



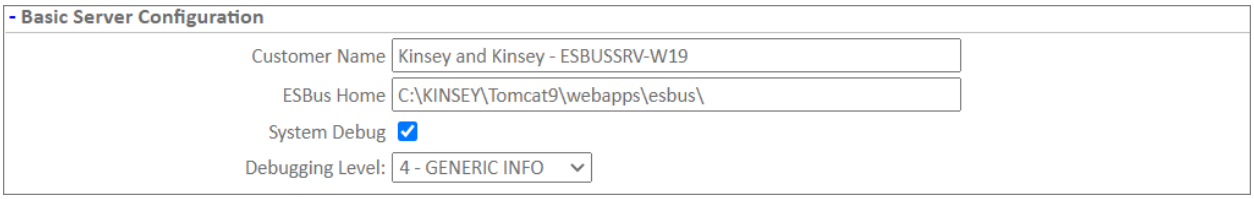
Select the Administration tab to log into the Admin page



Enter your administrative User name and Password

Configuration

Basic Server Configuration



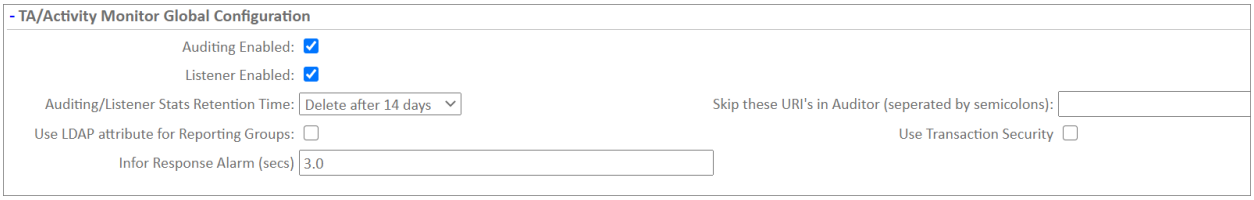
The only options you may want to change on this form pertan to the Tomcat system debugging logs. You can turn System Debug on or off and set the Debugging Level. The higher the level the more detailed the logs will be.

Global Configuration

The global configuration option determine how long you want to keep history on any emailed reports. Reports are emailed based on their defined schedule. This includes Security reports SoD reports, Transaction Auditing reports and Security Audit reports.

Transaction Auditing Global Configuration

These options are only needed for customers who have purchased the Transaction Auditing or Activity Monitor (Listener) applications.



Auditing Enabled	Check this box if you want Transaction Auditing data saved. This flag only controls the storing of data. Refer to the installation guide on turning off the application.
Listener Enabled	Check this box if you want Listener data saved. This flag only controls the storing of data. Refer to the installation guide on turning off the application.
Stats Retention	Set the length of time you would like to retain TA and Listener statistics.
Skip URI's	Enter any URL's you would like skipped in the collection of data.

Segregation of Duties Global (SoD) Configuration (S3 only)

This option is only needed for customers who have purchased the Lawson S3 Segregation of Duties application. This does not apply to Landmark SoD.

The configuration option allows you to determine the function codes that will cause a violation with a policy. By default the system is set to A (add), C (change) and D (delete). This means that if an LS user has access to any one of these function codes on a form then the form could be in violation depending on the rules of the policy. Forms without the function codes defined in the function code violation field are considered inquiry-only and treated the same as no-access.

SoD Function Code Violations	Enter the function codes that will cause a form to be in violation if active. The function codes entered here only pertain to the header on a form. Line code function codes are not checked when looking for SoD violations.
Role(s) to skip SoD Report	You can configure the application to skip LS admin roles so they do not continually show on the SoD reports.
SecClasses to skip SoD Report	You can configure the application to skip LAUA admin security classes so they do not continually show on the SoD reports.

Use database for LS SoD (not LDAP) – Check this option if you want the SoD reports to use the Kinsey LS SQL database to check for SoD violations or leave this option unchecked to if you want SoD to check LDAP directly. This option is checked by default.

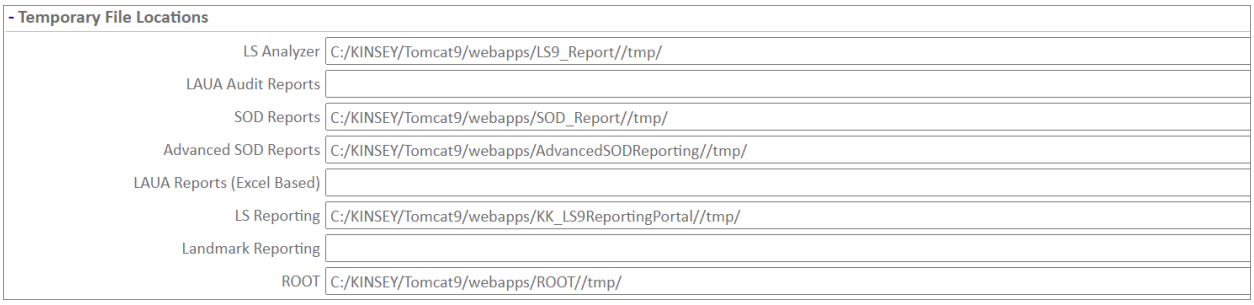
Treat conditional logic as NO_ACCESS – by default any form using conditional logic to determine access will be treated as having A,C, or D acces. If you want forms with conditional logic to be teated as through a user will not have A,C, or D access then check this box and the conditional logic forms will not be flagged in violation of a policy.

Note: The SoD application will use the security settings found in the profile name field defined under LS Security Configuration (LDAP Profile)

Note: The function codes A, C and D are default settings. The actual function codes used by the SoD application are defined in the SoD Function Code Violations field.

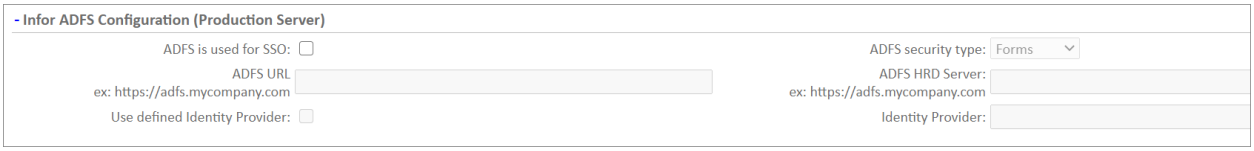
Temporary File Locations

This information will be configured on installation. Temporary files are maintained on the server used for the Kinsey application. For questions please contact Kinsey technical support.



Infor ADFS Configurtation (Production Server)

The configuration is defined by Kinsey on installation and should not be changed with contacting Kinsey support.



Lawson Configuration Production Server

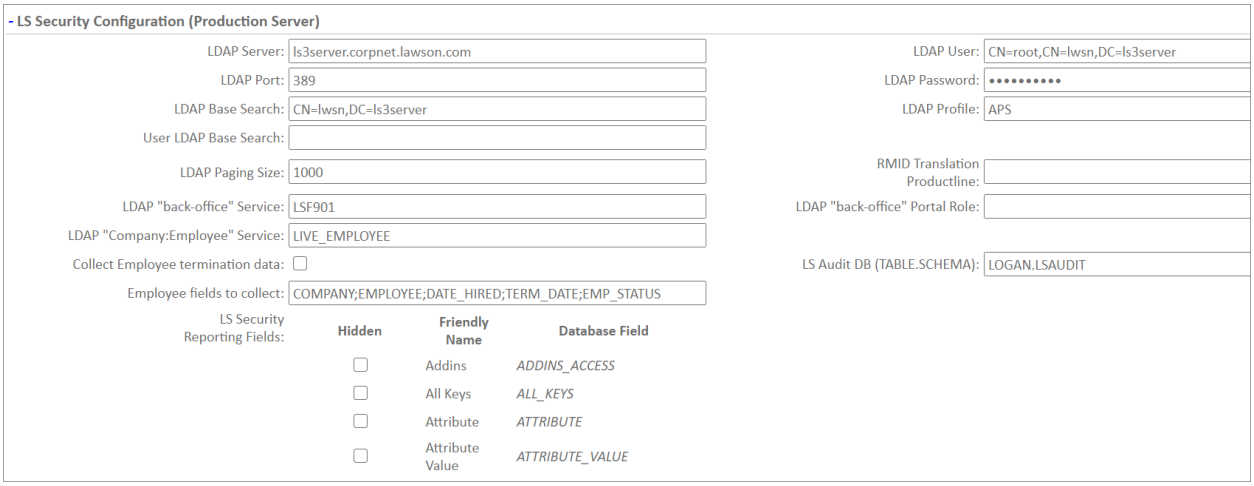
The configuration is defined by Kinsey on installation and should not be changed with contacting Kinsey support.

The following fields may occastionally need to be updated

Lawson Product Line	Enter the Production product line
Web Server	Enter the Web Server URL
Web User	This is the system admin user used to retrieve all security and transactional data.
Web Password	Enter the Web User password
Security Model	The Security Model checkbox is used to control the security model available when running SoD reports.

LS Security Configuration (Production Server)

The configuration is defined by Kinsey on installation and should not be changed with contacting Kinsey support.



The follow fields may occastionally need to be updated

LDAP Server	Enter the server ID
LDAP User	Enter the user ID of a read-only LDAP user
LDAP Password	Ente the read-only users password
LDAP Profile	Enter the default LDAP Profile for reporting purposes.
Employee fields	Changing the field names will have an adverse affect on the Terminate Employee LS Report. If you need additional fields pulled from Lawson contact Kinsey support for more infomation.
Reporting Fields	The security reports will include the fields displayed on the configuration screen. To hide fields by default from the report check the hidden check box next to the field name. You will have the option of overriding the default when you create the report.

Landmark Configuration (Prod)

The configuration is defined by Kinsey on installation and should not be changed with contacting Kinsey support.

Infor ADFS Configuration (Test Server)

The configuration is defined by Kinsey on installation and should not be changed with contacting Kinsey support.

Lawson Configuration (Test Server)

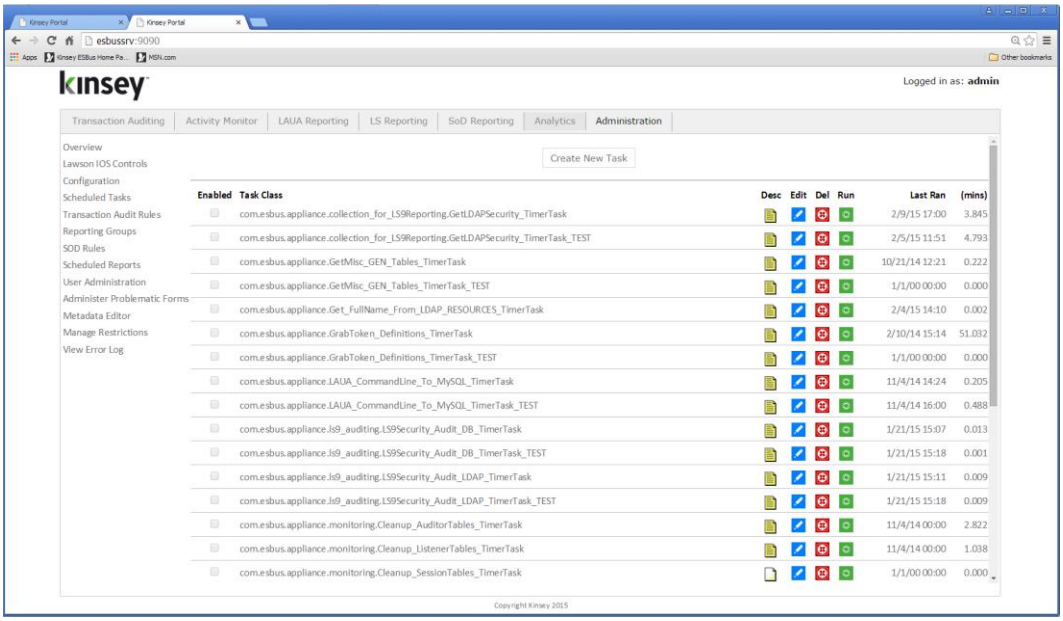
Refer to the Lawson Configuration Production Server instructions for more information.

LS Security Configuration (TEST Server)

Refer to the LS Production Server instructions for more information.

Scheduled Tasks

The scheduled tasks option allows you to maintain schedules or run on demand the tasks that retrieve and purge data from the reporting databases.



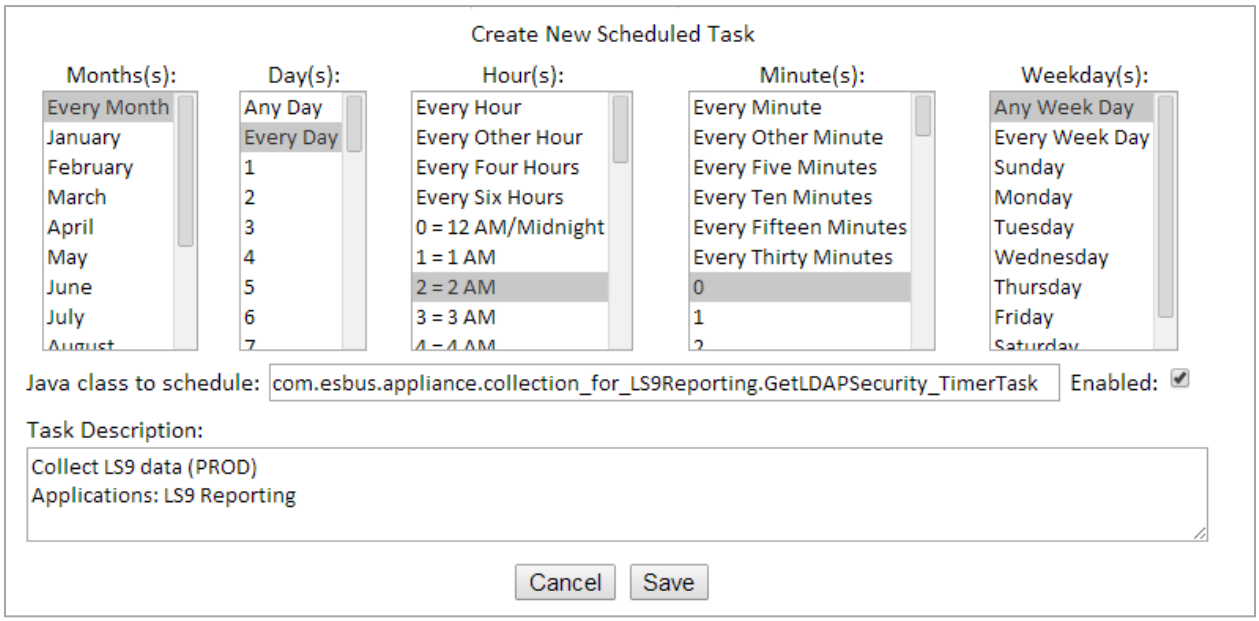
On Demand Tasks

The task can be run on demand as needed. You should consult Kinsey support prior to running any task not included in the list below:

Task	*Data collected*
Collect LS Auditing data (using ERP HTTP Call) (PROD)	Changes to security settings-Prod
Collect LS Auditing data (using ERP HTTP Call) (TEST)	Changes to security settings-Test
Generate SoD menu graphs	SoD Dashboard graphs
LS LDAP data collection (PROD)	S3 Security data-Prod
LS LDAP data collection (TEST)	S3 Security data-Test
Landmark Security data collection (PROD)	Landmark Security data-Prod

Landmark Security data collection (TEST	Landmark Security data-Test
Snapshot - Landmark data collection (PROD)	
Snapshot - Landmark data collection (TEST)	
Snapshot - Landmark Security data collection (PROD)	Landmark Security data-Prod
Snapshot - Landmark Security data collection (TEST)	Landmark Security data-Test
Snapshot - LS LDAP data collection (PROD)	S3 Security data-Prod
Snapshot - LS LDAP data collection (TEST)	S3 Security data-Test

Defining a Schedule



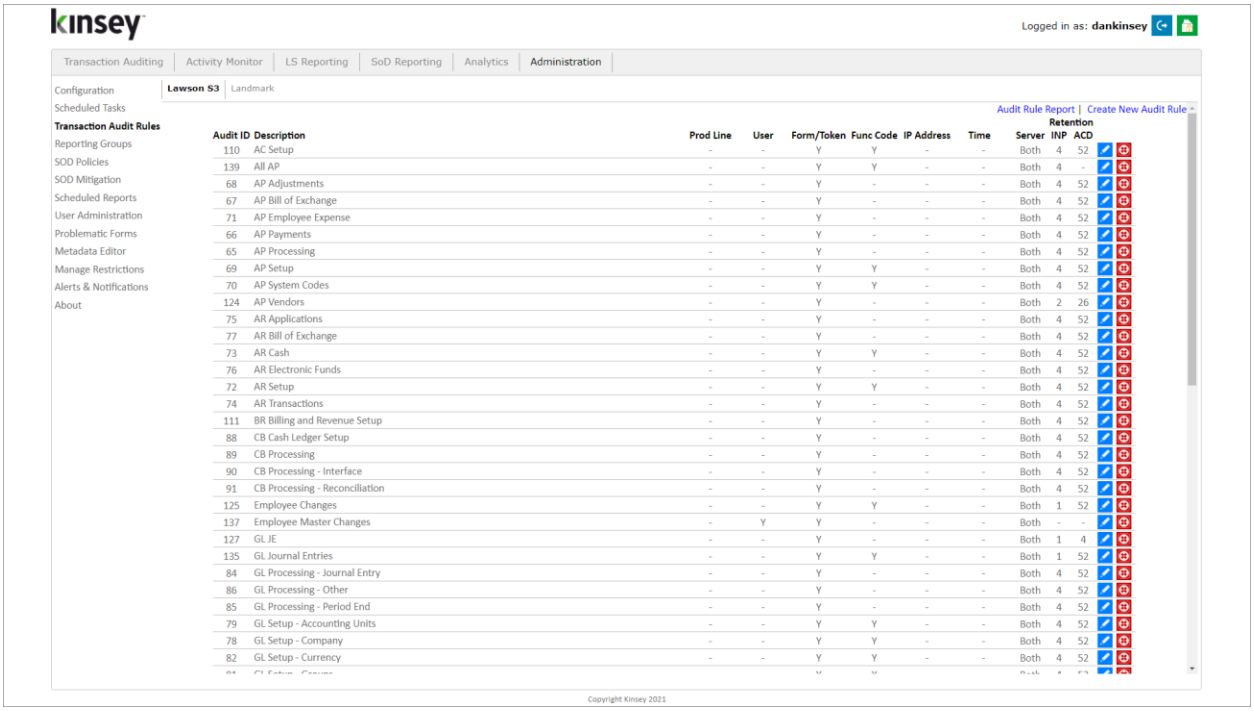
Select the **Edit** icon next to the process you want to schedule.

Month(s)	Select a month or every month
Day(s)	Select the day of the month to run the process
Hour(s)	Select the time of day to run the process. The process can be run based on increments starting 12:00am.
Minute(s)	Select the minutes past the hour or the minutes in increments based on the starting hour selected.
Weekday(s)	Select the day of the week that you want to run the process.

Note: You can use either the Day(s) or Weekday(s) criteria but not both. When using Day(s) set the Weekday(s) option to 'Any Week Day'. When using Weekday(s) set the Days(s) option to 'Any Day'

Transaction Audit Rules

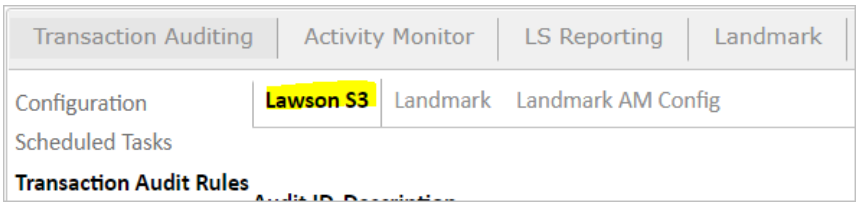
From the Adminstrative page select ”Transaction Audit Rules”. The existing rules will be displayed on one of two tabs for either Lawson S3 or Landmark (CloudSuite). Use the icons next to the report name to either edit or delete the audit rule. To add a new rule select the ”Create New Audit Rule” link in the top right corner.



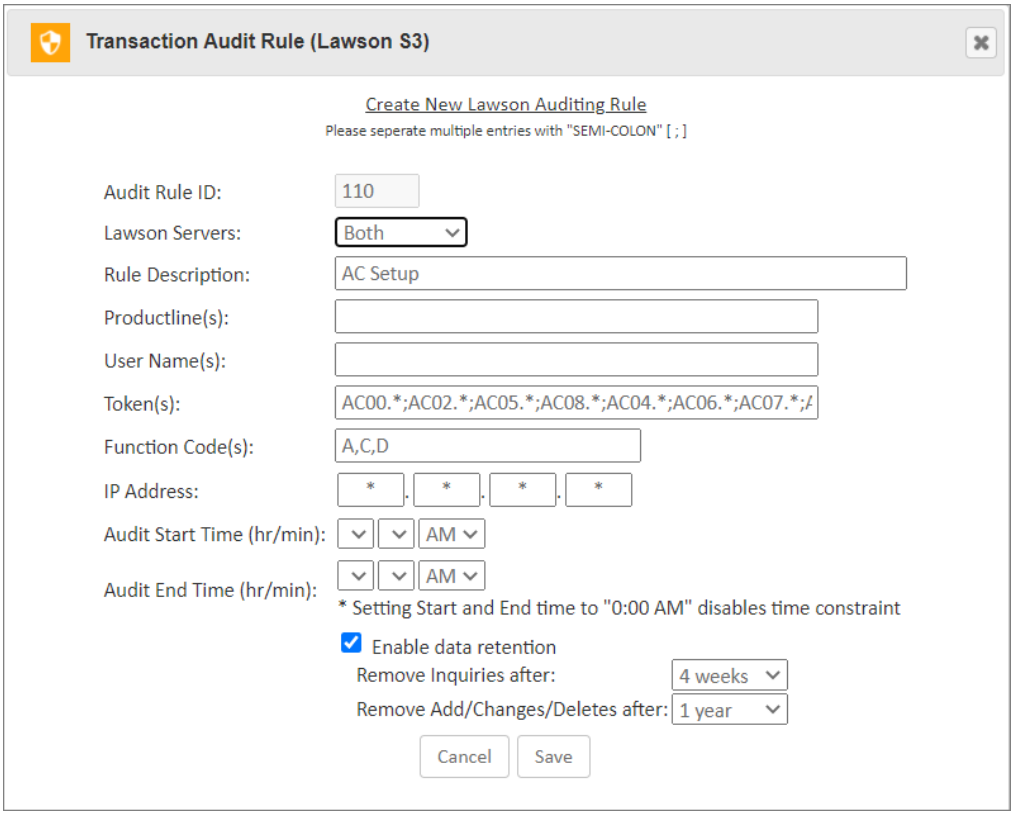
For all new rules the system will automatically assign an Audit Rule ID. This ID can be used in the selection criteria when setting up reports. This is helpful of you are setting up a group of tokens (forms) or a group of users that you want to audit. When you create a report you can simply request a query of all records matching the Audit Trail ID instead of creating criteria to match user names or token ID’s.

Creating or Changing an Audit Rule for Lawson S3

Start by selecting the Lawson S3 tab a list of existing S3 defined audit rules will be displayed.



To edit an audit rule click on the blue pencil icon next to an existing rule or to create a new rule select the 'Create New Audit Rule" in the upper right corner of the screen.



Audit Rule ID:	Automatically assigned
Lawson Servers:	Select the server you would like to audit
Rule Description:	Enter a description describing the purpose of the audit
Product Lines:	Enter the Product Line(s) you would like to audit
User Names:	Enter a list of users you would like to audit. Enter the users Lawson login ID as the User Name. To specify multiple users put a semicolon between each name. Leaving the field blank will automatically audit all Lawson Users.

Tokens: Enter a list of token or form names you would like to audit. To specify multiple tokens put a semicolon between each token name. For example HR11; AP10; GL20. Leaving the field blank will automatically audit all Lawson tokens.
Hint: The application will match token names based on the number of characters entered. For example if you enter "AP1" the system will audit all tokens beginning with AP1 (AP10.1, AP10.2, AP11.1, AP12, et.)

Function Codes: Enter the Function Code you would like to audit. Leaving the field blank will automatically audit all Lawson Function Codes.

IP Address: Enter the IP address that you want to audit. The application will match the originating IP address with the address entered from left to right. For example if you enter 192.168 and leave the 3rd and 4th segment blank the system will pick up all transaction from IP addresses matching the first 6 digits.

Audit Start Time: Enter the starting time for the audit to start capturing activity.

Audit End Time: Enter the ending time for the audit to stop capturing activity.

Enable Data Retention:
Selecting this option will allow you to set data retention policies for the data capture in this audit. If you do not set data retention policies all data will be kept indefinetely. Valid options are Never, 1, 2,4, 13, 26 & 52 weeks.

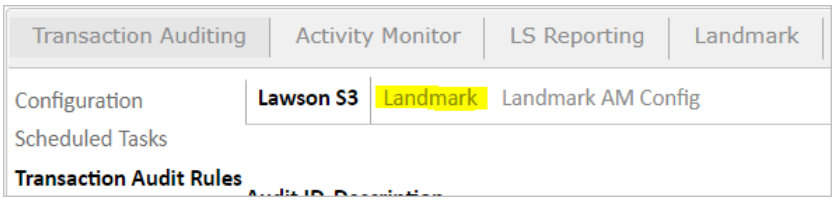
Remove Inquiries After:
Select the time period that you want to keep all data inquiry records. This will include function codes '(I)nquiry, (N)ext, (P)revious,(+) Page down (-) Page up.

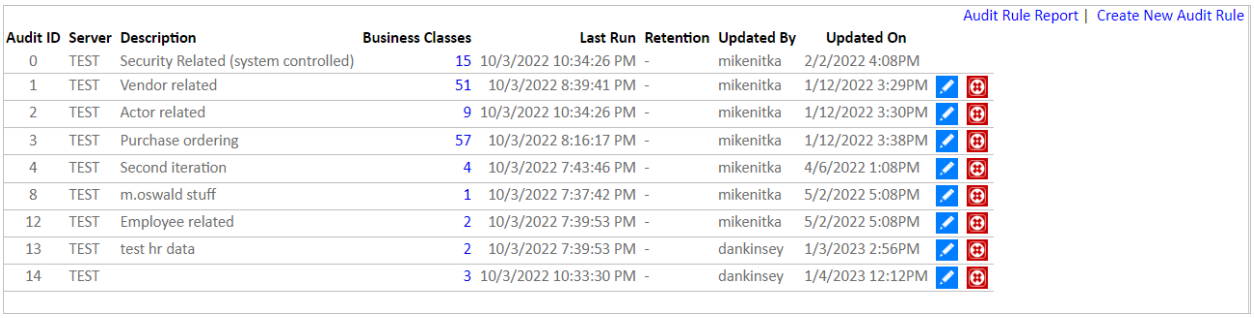
Remove Add/Change/Deletes after:
Enter the time period that you want to keep all non-inquire records.

Select **SAVE** to save your entry.

Creating, Changing or Deleting an Audit Rule for CloudSuite (Landmark)

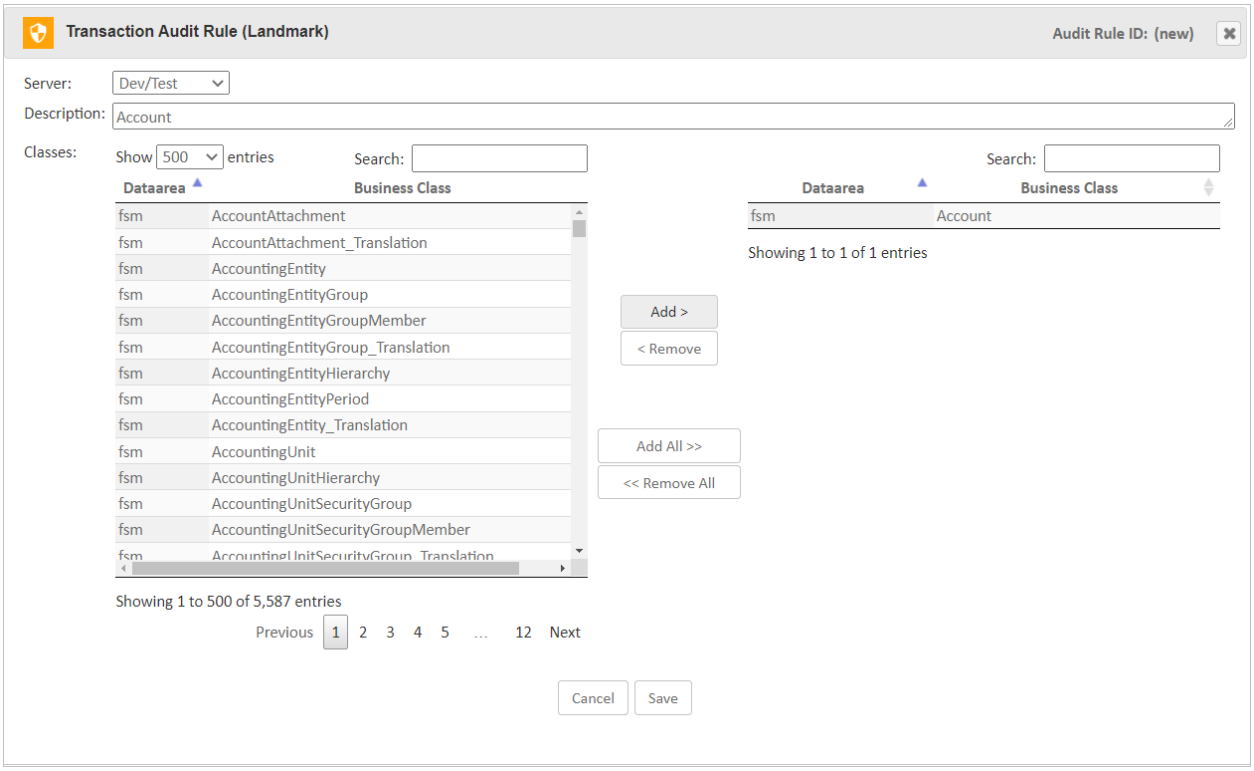
Start by selecting the Landmark tab and a list of the existing defined Landmark audit will be displayed.





Audit ID	Server	Description	Business Classes	Last Run	Retention	Updated By	Updated On
0	TEST	Security Related (system controlled)	15	10/3/2022 10:34:26 PM	-	mikenitka	2/2/2022 4:08PM
1	TEST	Vendor related	51	10/3/2022 8:39:41 PM	-	mikenitka	1/12/2022 3:29PM
2	TEST	Actor related	9	10/3/2022 10:34:26 PM	-	mikenitka	1/12/2022 3:30PM
3	TEST	Purchase ordering	57	10/3/2022 8:16:17 PM	-	mikenitka	1/12/2022 3:38PM
4	TEST	Second iteration	4	10/3/2022 7:43:46 PM	-	mikenitka	4/6/2022 1:08PM
8	TEST	m.oswald stuff	1	10/3/2022 7:37:42 PM	-	mikenitka	5/2/2022 5:08PM
12	TEST	Employee related	2	10/3/2022 7:39:53 PM	-	mikenitka	5/2/2022 5:08PM
13	TEST	test hr data	2	10/3/2022 7:39:53 PM	-	dankinsey	1/3/2023 2:56PM
14	TEST		3	10/3/2022 10:33:30 PM	-	dankinsey	1/4/2023 12:12PM

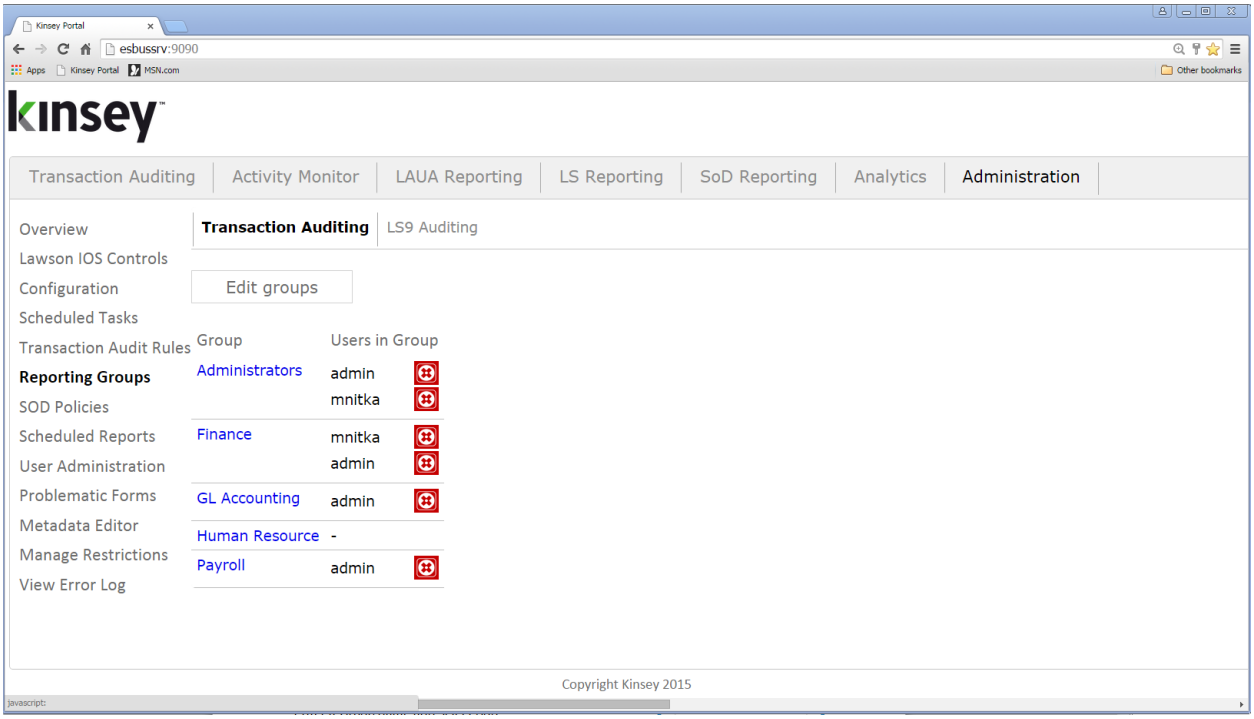
To edit an audit rule click on the blue pencil icon next to an existing rule, to delete a rule simply select the delete red icon or to create a new rule select the '**Create New Audit Rule**" in the upper right corner of the screen.



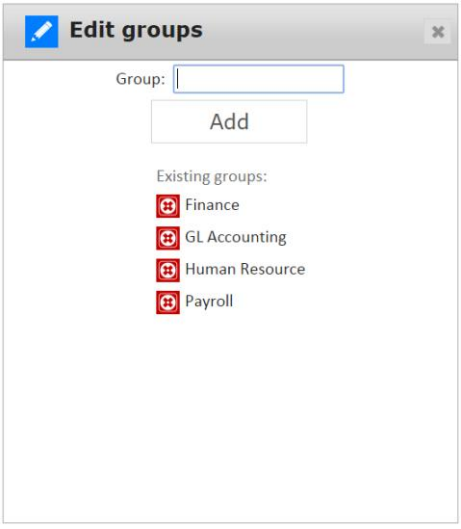
Server	Select the approiate server from the dropdown option.
Description	Enter the description or reason on why this audit is being defined. This is for references purposes only.
Classes	A list of all available classes will be displayed. Select a range of classes using the "shift" key, individual class using the "ctrl" key or simply click and add to add one at a time. Use the Search box if filter the list of Business Classes.
Save	Select the Save button to save your selections

Reporting Groups

Reporting Groups provide additional security for saved Transaction Audit and LS Audit Reports. This system will only allow users to save or run reports within their own group or run reports from the shared group.



Select Reporting Groups from the left navigation pane. All users previously created under User Administration will be display.



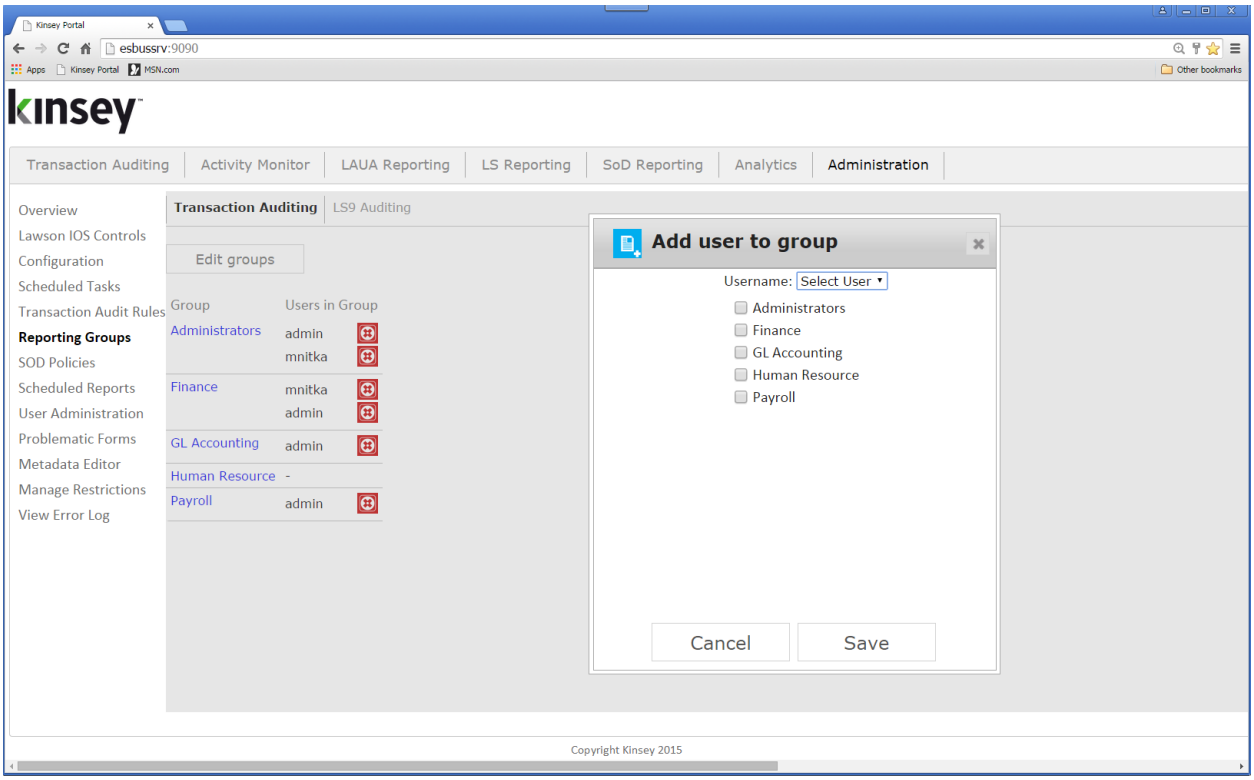
Creating or Deleting a New Group

To create new groups click on the Edit Group button.

Enter a Group name and select Add

To delete an existing Group select the red X next to the group name.

Assigning or Removing a User to a Group

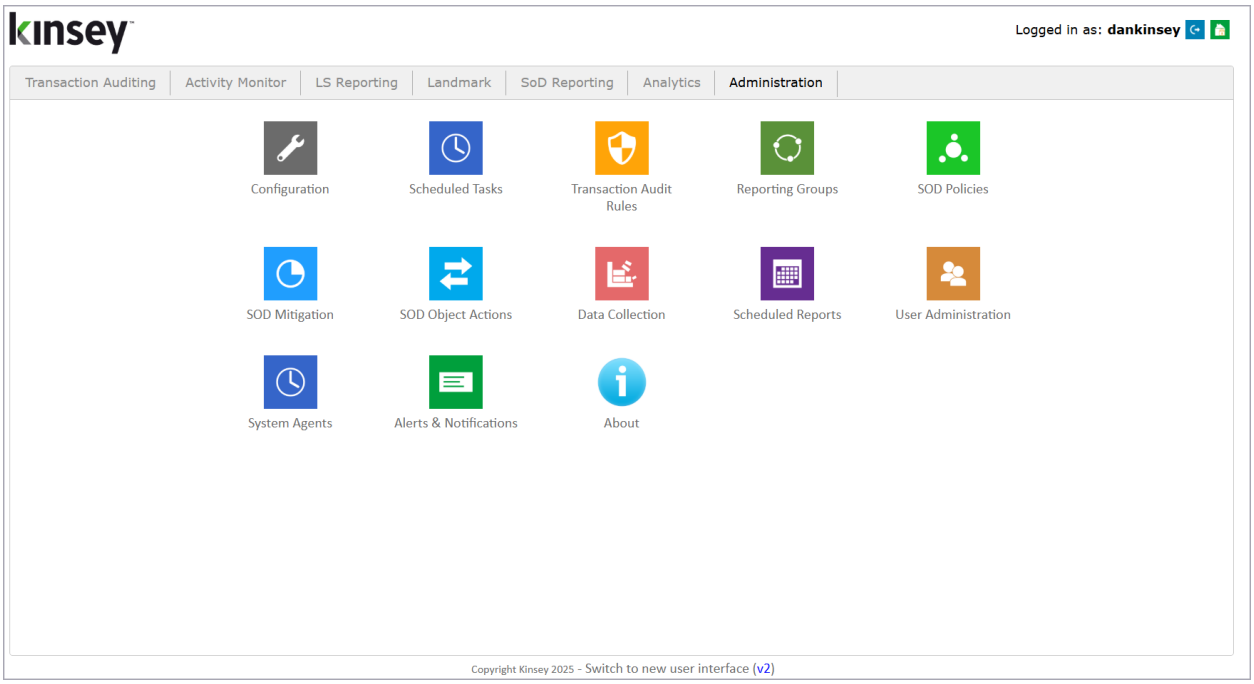


Click on any of the Group names to add a user to the group. To delete a user select the delete icon next to the user's name.

Any user added to the Administrators Group will be given full access to all reporting groups. This user is not considered an administrator for any other configuration purpose; this only allows the user to see all reports in all groups.

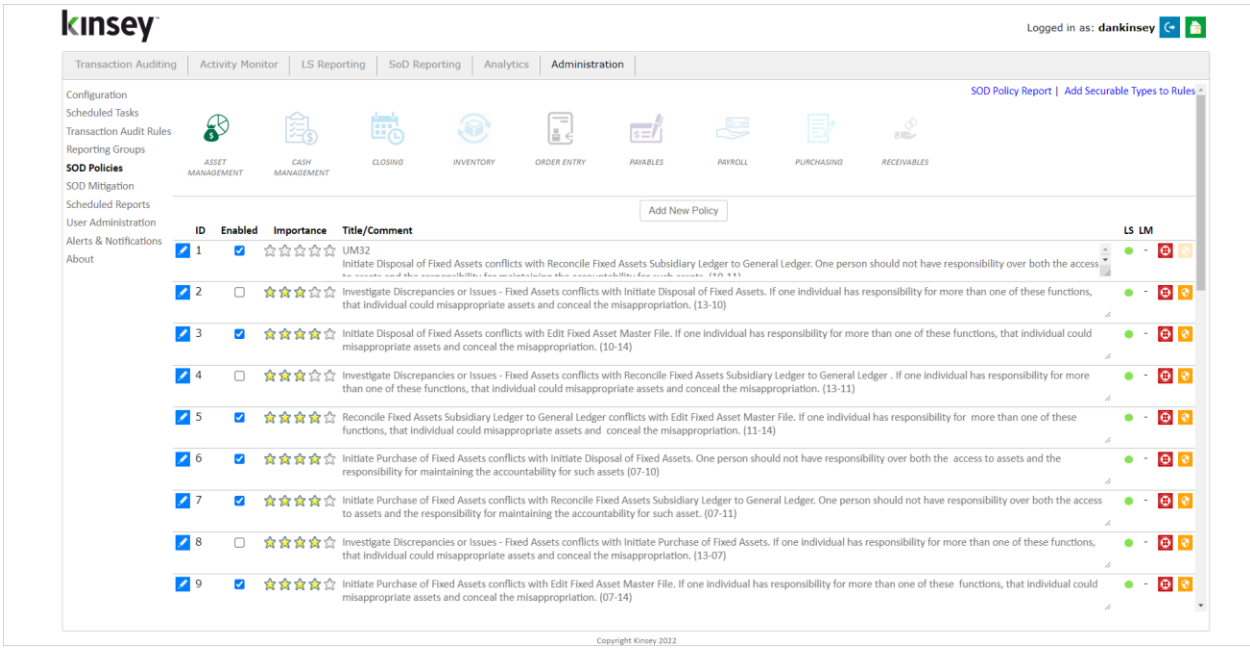
SOD Policy Maintenance

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



To add or change SoD policies start with the **Administration** Portal Page, then select the **SOD Policies** icon.

SoD Policies and Rules



The delivered policies are divided in to 9 categories. Additional categories can be added to maintain any other policies that do not fit into one of the existing categories. The dot next to the policy indicates the application the policy pertains to. Green is for Lawson V10 (S3) and orange is for CloudSuite (Landmark).

Auditing a Policy (S3 only)

Each policy has rules assigned based on conflicting objects. For Lawson V10 (S3) the rules are based on token's (forms), for Landmark they are set up for both Security Class and Business Clases. Clicking on the blue pencil edit button will display the objects that make up the SoD rule. You can quickly set up a Transaction Audit code for a specific SoD policy by clicking on the orange icon next to the policy description. The Transaction Auditing application is required to report on this activity.

Enabling/Disabling a Policy

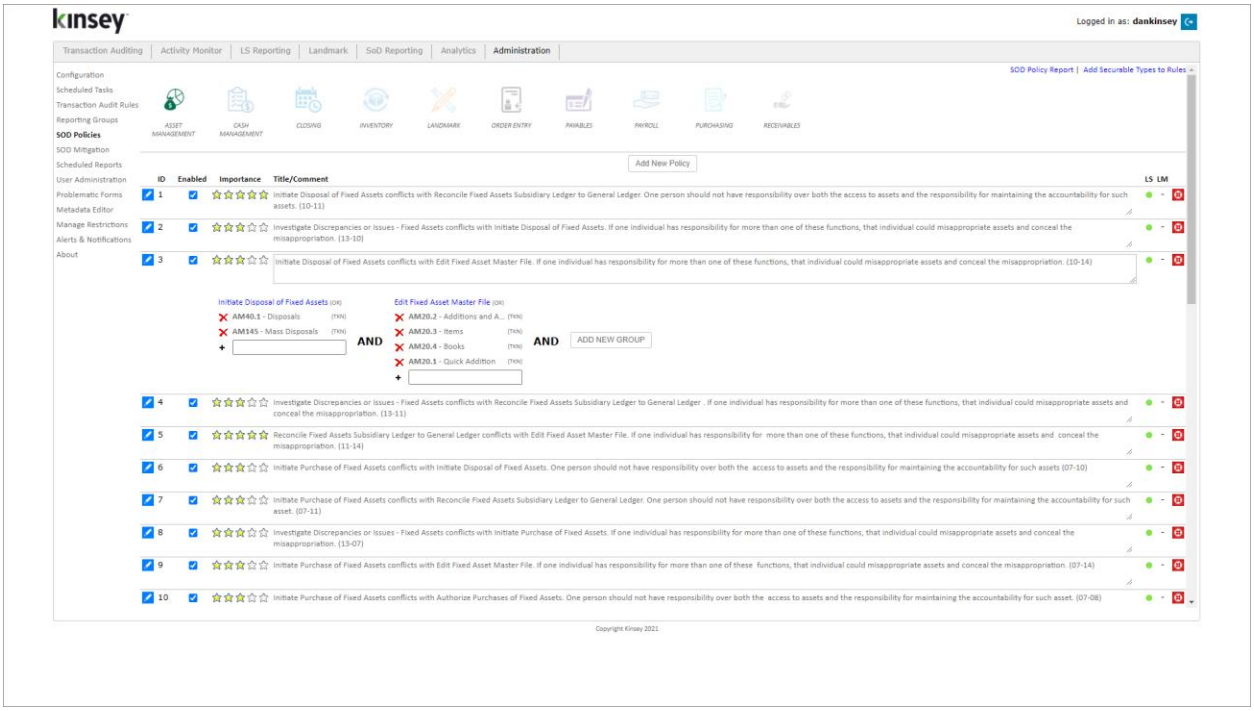
Each policy can be permanently disabled by un-checking the 'Enabled' check box. Any policy that is disabled will be removed from the SoD report. To enable a policy check the appropriate box next to the policy.

Rating a Policy's Level of Importance

The system will display the available categories and the individual policies. Each policy has a level of importance rating of 1 to 5 stars, with 5 being the most important. When the application is installed every policy received a 3 star rating. The rating is then used to filter the policies you need to review when you run the SoD report. To change the Importance levels simply click the appropriate star to increase or decrease the level.

Viewing or Editing a Policy

You can view or change the object assignments for any of the pre-built policies by clicking on the View/Edit link.



Every pre-built policy is created using 2 object groups. The groups are joined using AND logic, but the objects within each group are evaluated using OR logic. By combining AND/OR logic we are able to combine what would traditionally require multiple rules into one rule.

The example above shows 2 groups with 2 and 4 objects respectfully. When evaluating this policy the application will validate your security setting against 8 rules.

The user is in violation of the policy if that have at least A,C or D access to:

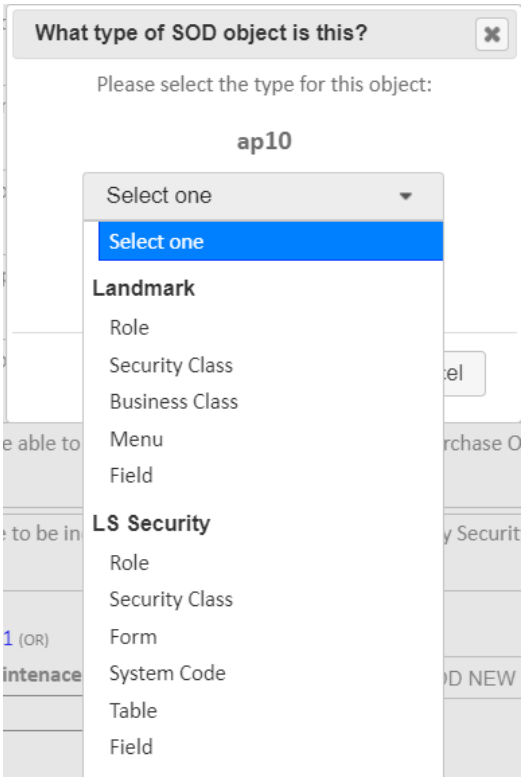
AM40.1 and AM20.1 or
AM40.1 and AM20.3 or
AP40.1 and AM20.4 or
AP40.1 and AM2-.1 or
AM145 and AM20.1 or
AM145 and AM20.3 or
AP145 and AM20.4 or
AP145 and AM2-.1

If any of these conditions are true the policy is considered to be in violation.

Note: Only objects with 'Update' access will cause a violation to occur. If just Inquiry functionality is granted for an object then the object is considered to have NO ACCESS when evaluation the SOD Policy.

Adding an Object to an existing policy (S3)

To add an object to an existing policy, type the object ID in the open cell under the appropriate group and click on the plus (+) sign left of the field. There are 6 types of objects you can add to an LS rule. Forms (tokens), Tables, System Codes, Roles, Security Classes or Fields. When the object ID is entered the system will attempt to identify the object type. If the field type cannot be auto identified you will be prompted to select the type of ID entered.

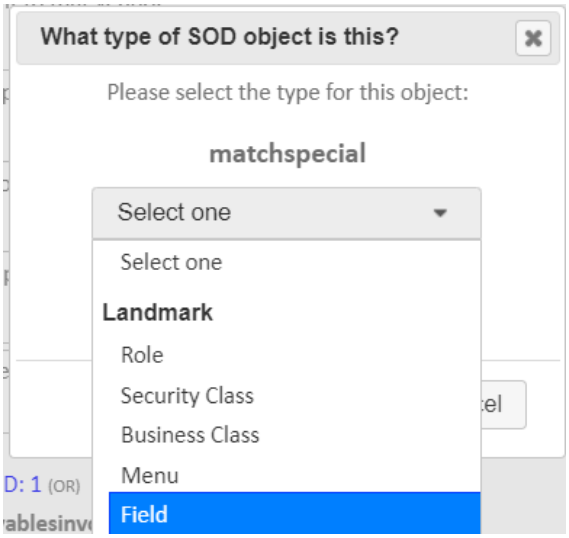


Any combination of objects can be used when defining a policy. If you enter a Form (token) ID you can use a wild card ('*') to define a series of forms. For example AP20.* will look for AP20.1, AP20.2, AP20.3, etc.

Note: When using wild cards to identify on-line tokens be sure to include the '' after the fifth character (.). In the example above if the token is entered as AP20* instead of AP20.* you will be including all of the AP200 reports in the rule.*

Adding an Object to an existing policy (Landmark)

To add an object to an existing policy type the object ID in the open cell under the appropriate group and click on the plus (+) sign left of the field. There are 3 types of objects you can add to a rule. Business Classes, Roles and Security Classes. When the object ID is entered the system will attempt to identify the object type. If the field type cannot be auto identified you will be prompted to select the type of ID entered.



Deleting an Object from an existing policy

To delete the assignment of an object simply click on the delete icon next to the object name.

Adding a Group to an existing policy

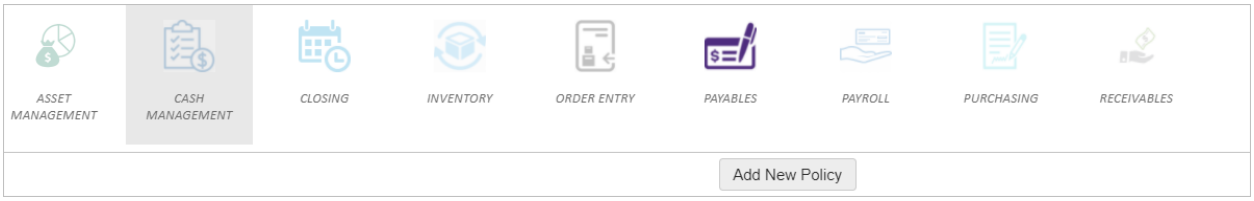
To add a new Group to a policy click on the ADD NEW GROUP button and fill in the appropriate object ID's.

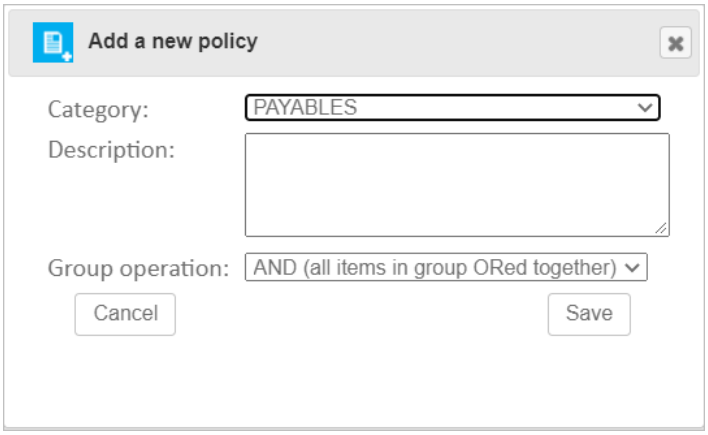
Deleting a Group from an existing policy

To delete a Group simply delete every object in the group and refresh your browser page.

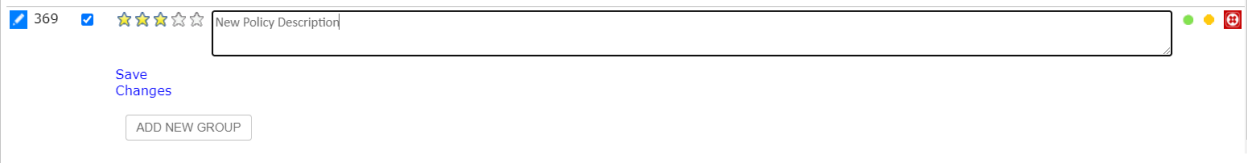
Creating a New Policy

You can create an unlimited number of new policies and assign them to any category. To add a new policy click on the Add New Policy link in the top center of the SoD screen.





You need to enter a policy description, category and group operation prior to entering the objects related to the rule. The rule group will be set to AND by default. This is the setting used for all of the pre-built policies. You can however use OR logic between the groups. By choosing OR logic, all of the objects in the group will share the AND conjunction.



Start by adding a new group and entering the object ID's in Group 0 as described in the "Adding an Object" section. You can then Add a New Group and assign the appropriate objects to Group ID 1.

Note: When you are finished building your new policy remember to make sure it is enabled and star rated.

Deleting a Policy

To remove a policy permanently you can either delete every object assigned to the policy and refresh your browser page or click on the red delete icon next to the policy description.

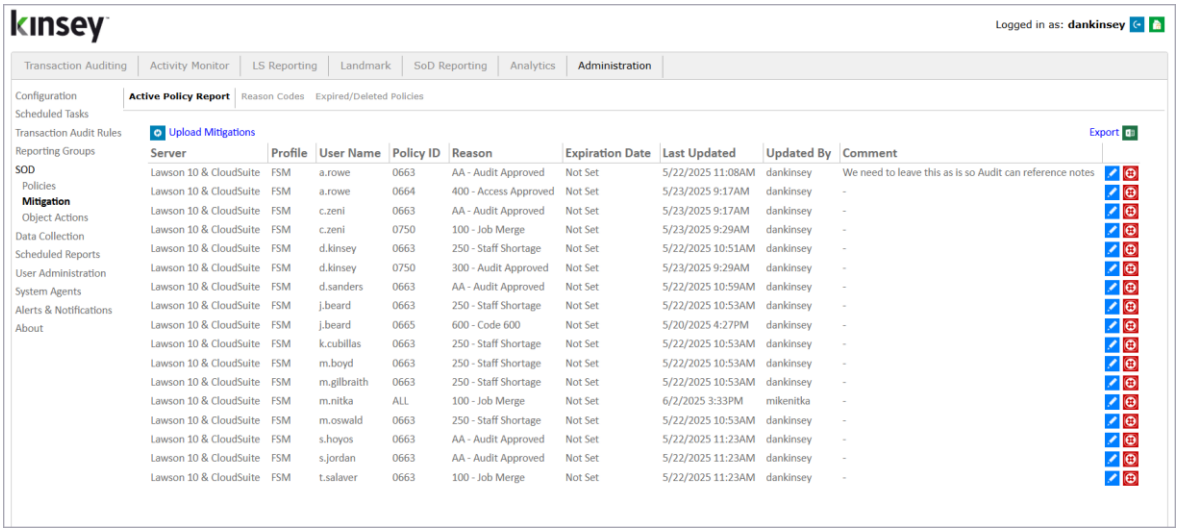
SOD Mitigation

Mitigations are used to explain and exempt a policy violation for a user. Mitigations can be assigned on either the HTML SOD Report or by using the MS Excel export. Refer to the SOD User's guide on how to assigned user-policy mitigations.

The SOD Admin Mitigation feature has 3 options.

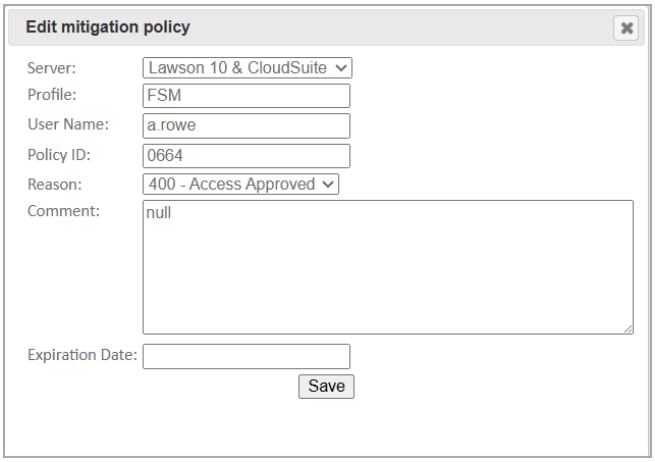
- A list of current mitigations by User
- A list of mitigation reason codes
- A list of expired or deleted mitigations

Active Policies Report



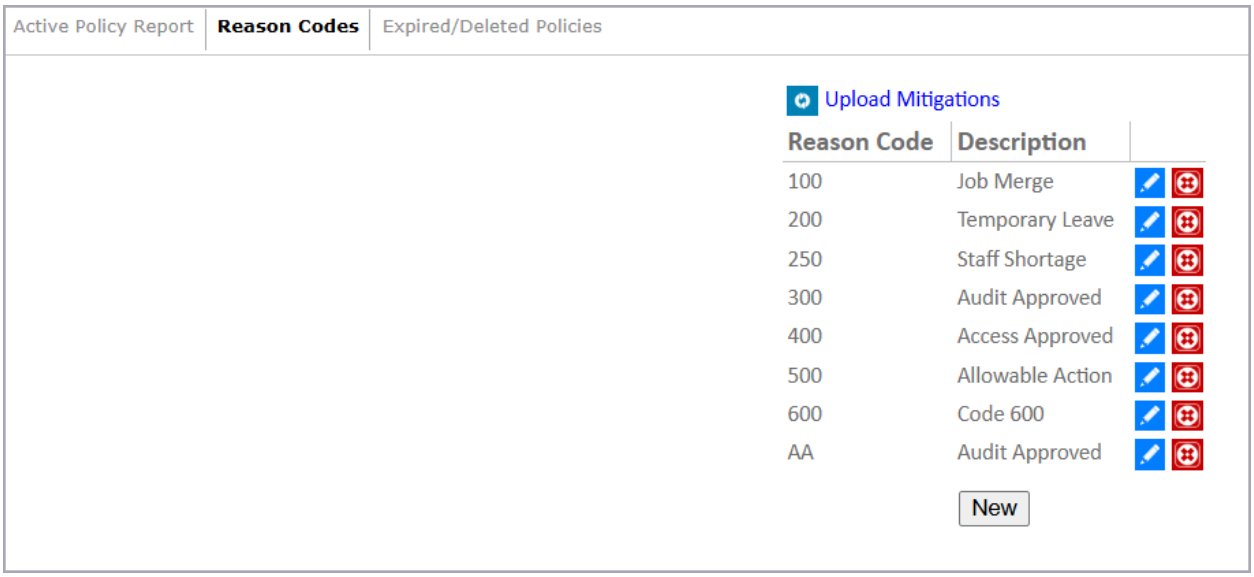
The active policy screen provides the option to export a list of mitigations, edit the mitigation or delete the mitigation.

To edit the mitigation select the blue pencil icon and change as needed.



Reason Codes

Reason codes provide a brief justification for the mitigation. The code is assigned when the mitigation is applied. Refer to the SOD User's guide on how to assigned user-policy mitigations.

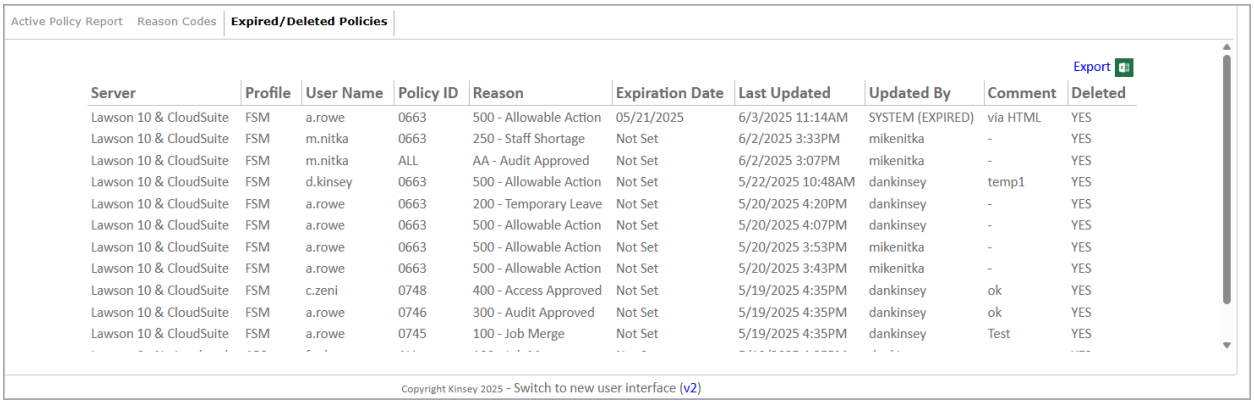


You can add a New code, delete an existing code or change the description of a code.

Note: Deleting a code will not remove it from an existing mitigation.

Expired/Deleted Policies

The Expired/Deleted Policies screen provides the option to export a list of all deleted mitigations.

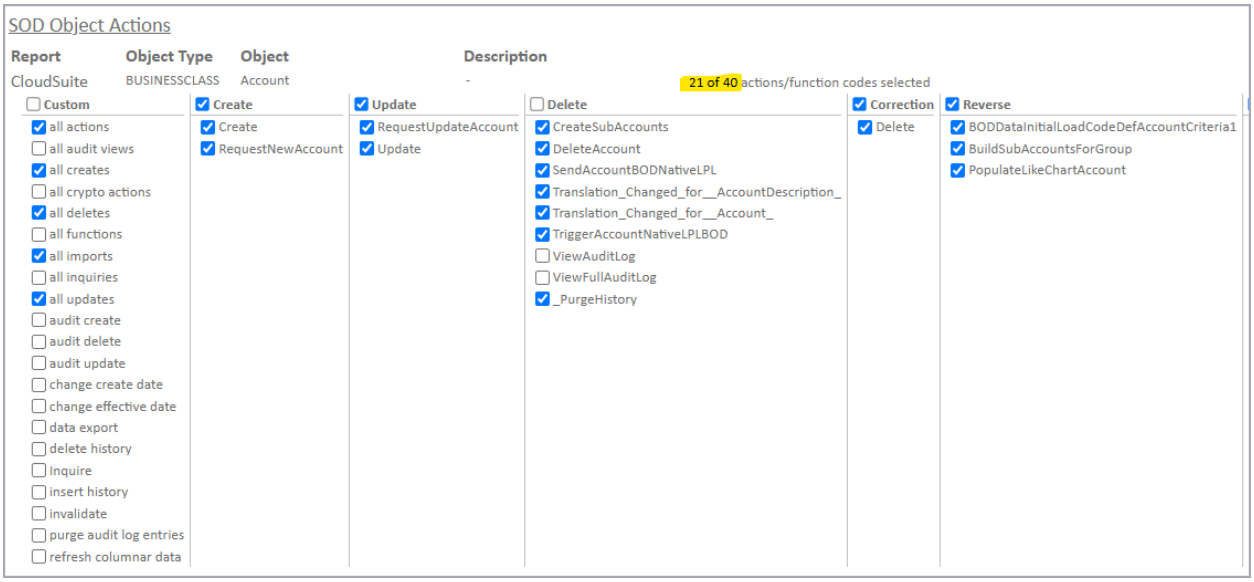


SOD Object Actions (Landmark)

Using the URL provided during the installation launch the Kinsey Portal home page. When using Business Classes in a rule the level of access available is based on the security settings in the Security Class LPL for the Business Class object.

One the Kinsey portal Administration page there is an option for SOD Object Actions. The “actions” that can be executed on the Business Class are more in depth that found in Lawson V10 (S3).

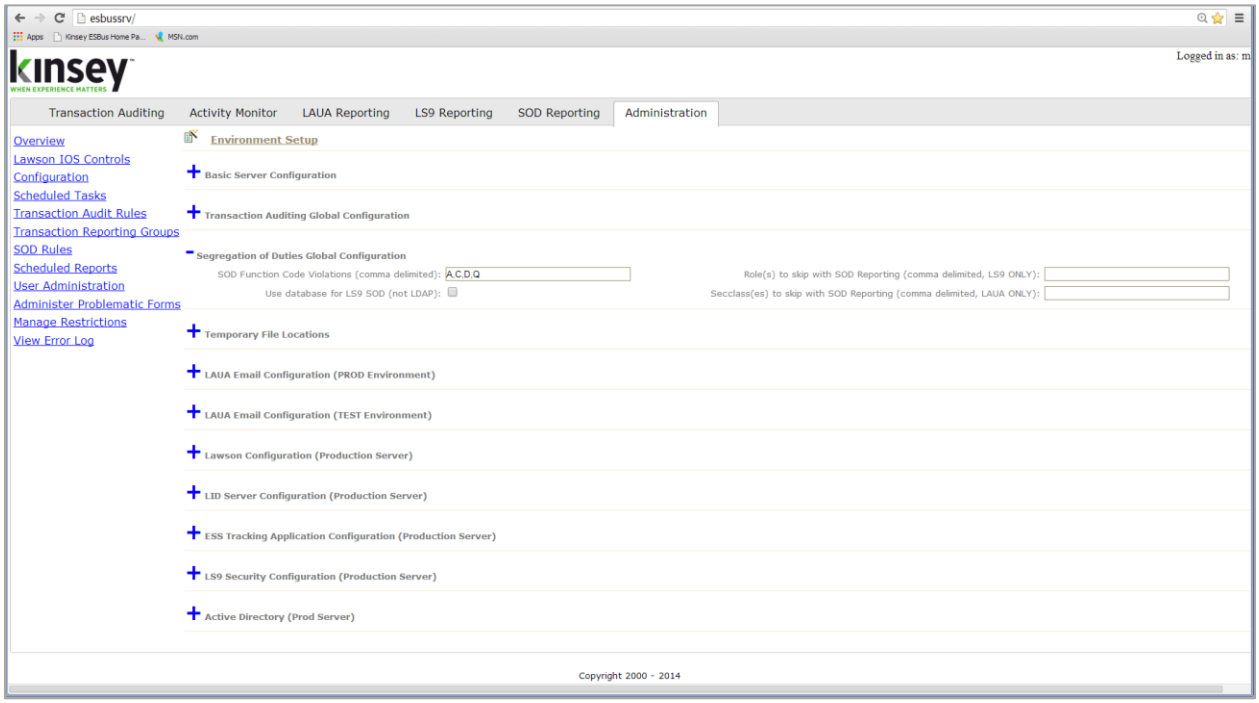
Every Business Class defined in an SOD policy will appear on this page. Clicking on the action count will expand the section. The actions checked will be used to determine if the Business Class is in violation of a policy.



SOD Configuration

Lawson V10 (S3)

Using the URL provided during the installation launch the Kinsey Portal home page. The configuration option allows you to determine the function codes that will cause a violation with a policy. By default the system is set to A (add), C (change), D (delete) and Q (quick). This means that if an LS user has access to any one of these function codes on a form, then the form could be in violation depending on the rules of the policy. Forms without the function codes defined in the function code violation field are considered inquiry-only and treated the same as no-access.



To change the function code violations and role exclusions select **Configuration** from the **Administration** Portal page.

SoD Function Code Violations	Enter the function codes that will cause a form to be in violation if active. The function codes entered here only pertain to the header on a form. *Line code function codes are not checked when looking for SoD violations.*
Role(s) to skip SoD Report	You can configure the application to skip LS admin roles so they do not continually show on the SoD reports.

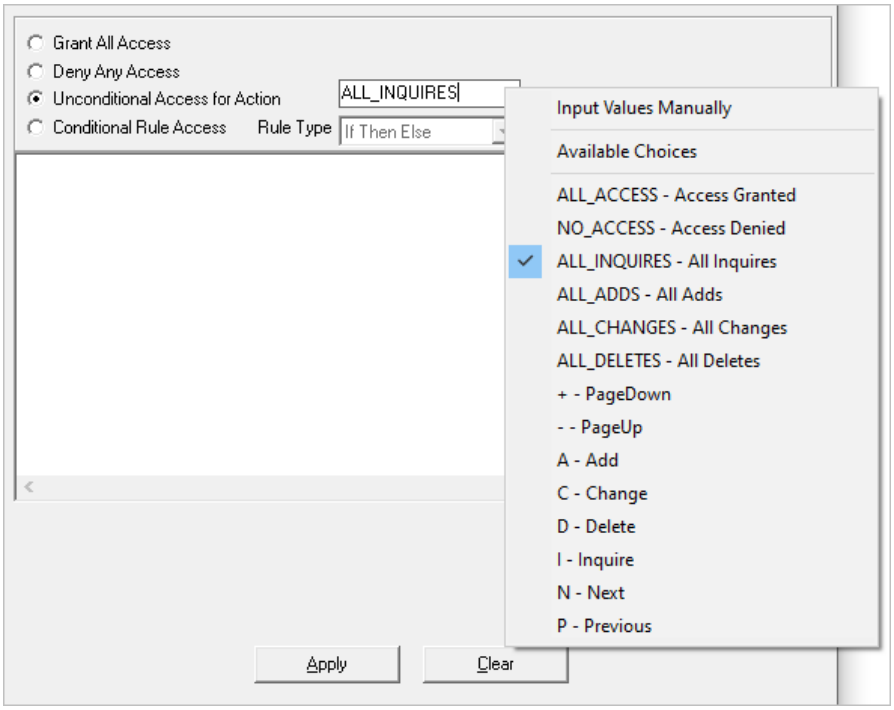
SecClasses to skip SoD Report	You can configure the application to skip LAUA admin security classes so they do not continually show on the SoD reports.

Use database for LS SOD (not LDAP) – this option should be checked.

Exceptions for Inquiry-Only Forms

Lawson Security

For LS, the process analyzes how access is granted. If a token is granted "All Access" then we treat it as a violation even if the only available function is an *inquiry*. However, if you put specific Function Codes in the "Unconditional Access for Action" (which actually means "Screen Actions Allowed") for the token we look at the actual rule.



On the screen example above, if I add INP+- to the token restriction any SoD violation goes away because we see this as inquiry-only. As far as Lawson is concerned, granting **All Access** on a form or assigning all of the available function codes for Unconditional Access rules has the same net effect on security.

Recap

S3 Rules

- By default, if you restrict access to FC's A, C and D on a token then it's considered Inquiry-only and will NOT cause a violation. Refer to the Administration Guide on how to add additional function codes to the restriction list.
- If a Token that only has Inquiry capability is defined under "Unconditional Access for Action" as INP+- then it will NOT cause a violation however if the rule is set to "All Access" it may result in an SoD violation.

Note: For Kinsey's SoD application, Inquiry-only is defined as a token that does not have A,C or D Function Codes assigned.

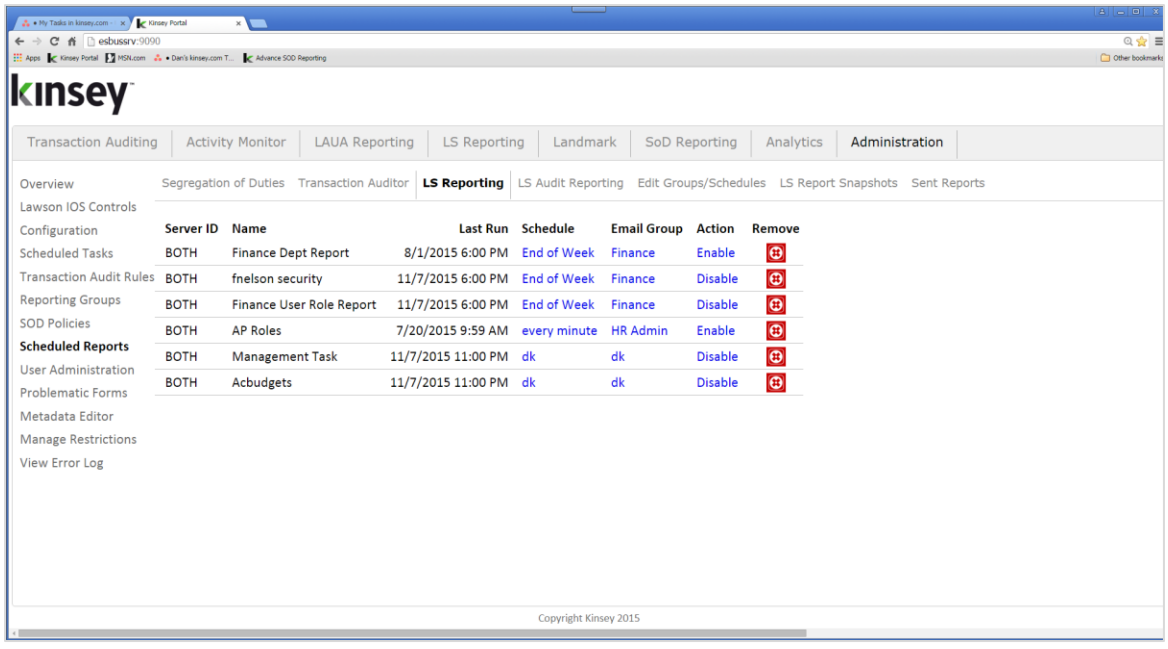
Note: The function codes A, C and D are default settings. The actual function codes used by the SoD application are defined in the SoD Function Code Violations field under the Segregation of Duties Global Configuration on the Administration page.

Scheduled Reports

The Scheduled Report option allows a administrator to Enable or Disable an existing schedule for Transaction Auditing, Security Auditing, Security Reporting, Security Auditing, and SoD Reports. You can also maintain the saved schedules and reporting groups through this option.

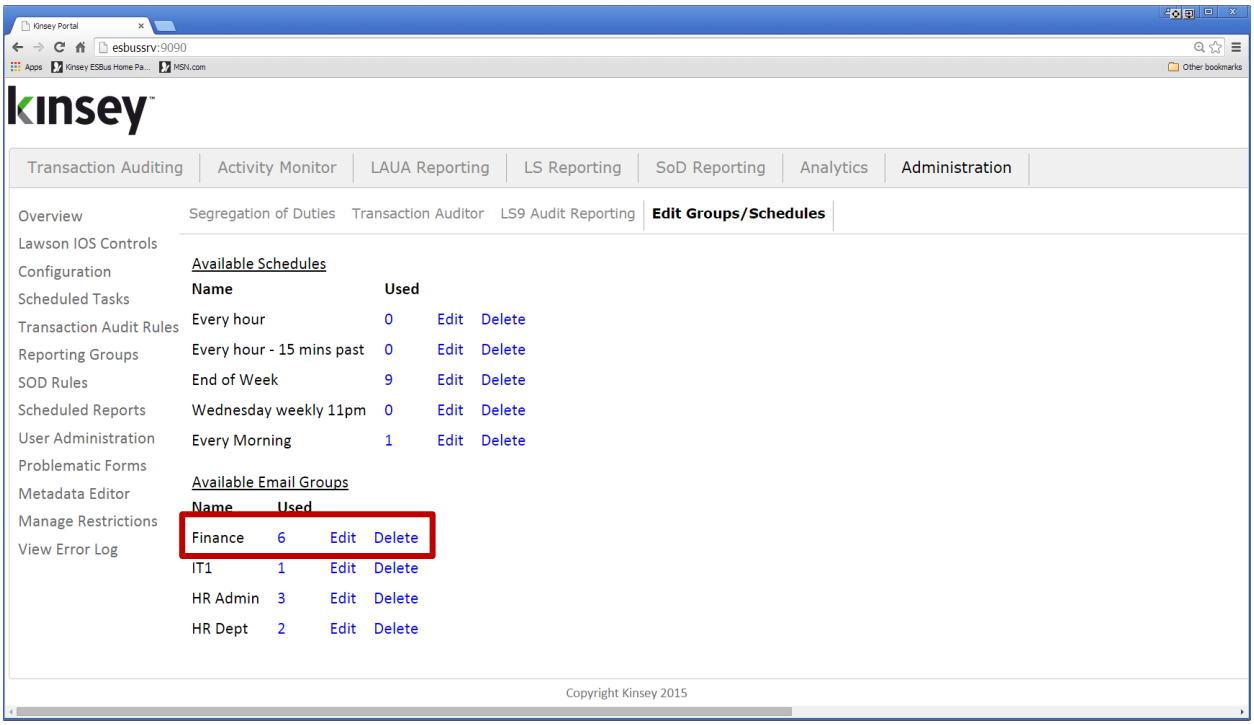
Enabling or Disabling a Scheduled Report

Using the Administrator tab on the home page select Scheduled Reports. The 'Action' column on the right provides the option to enable or disable a schedule. For example in order to enable a schedule you must select the ENABLE link. The link does NOT show the current status. The link indicates the action you want to take.

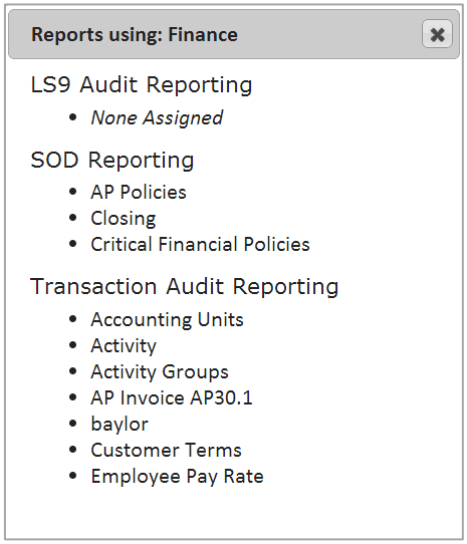


Editing Email Groups

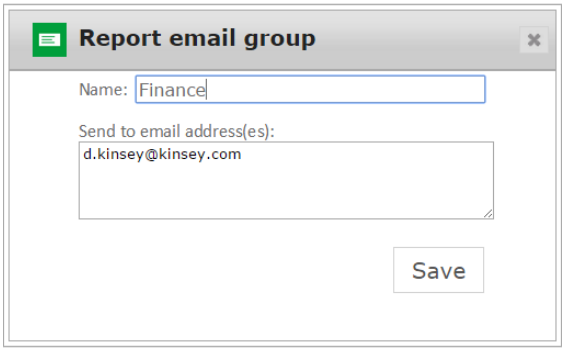
Select the Edit Groups/Schedules tab from the Administration > Scheduled Reports link. Email Groups hold a list of email addresses for report distribution. When a report is scheduled in either Transaction Auditing, Security Auditing or Segregation of Duties you can select an email group for automatic distribution.



The number to the right of the group indicates the number of reports assigned to this group. To view the current assignments simply click on the number.

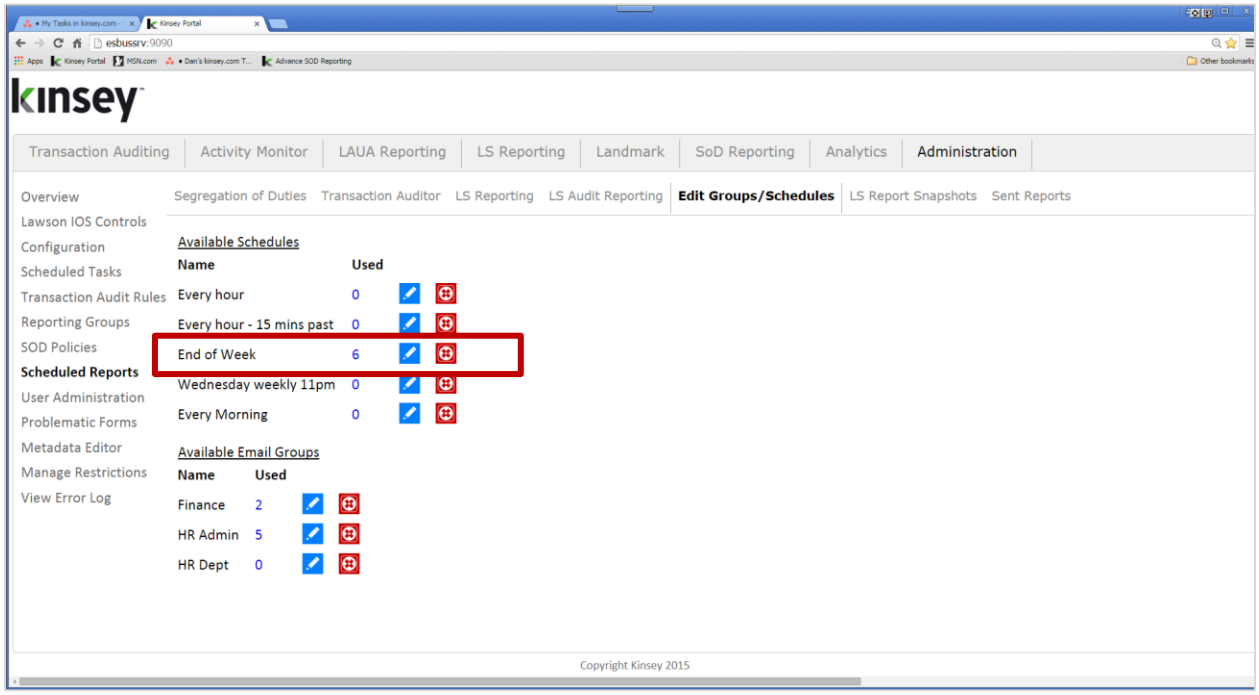


To change the email addresses asigned to the group select the Edit link.



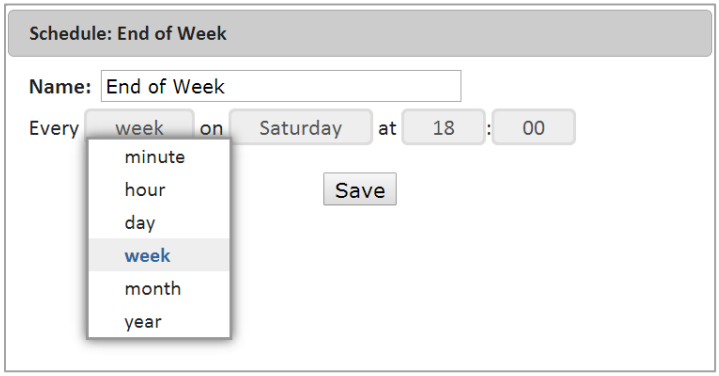
Editing Schedules

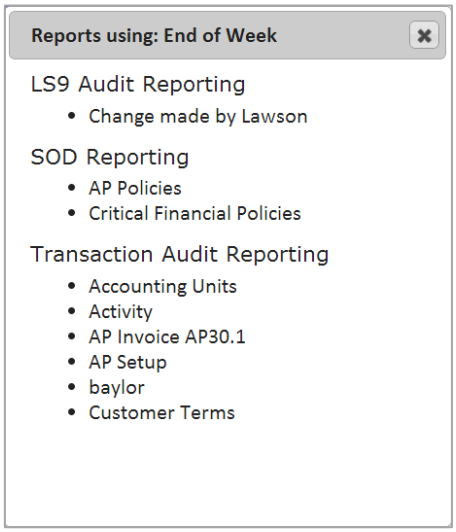
Select the Edit Groups/Schedules tab from the Administration > Scheduled reports link. Schedules are used to determine when reports are generated and distributed for Transaction Auditing, Security Auditing or Segregation of Duties.



The number to the right of the Schedule name indicates the number of reports assigned to this schedule. To view the current assignments simply click on the number.

To edit and existing schedule select the Edit link and make the appropriate changes to the Period, Date and Time.

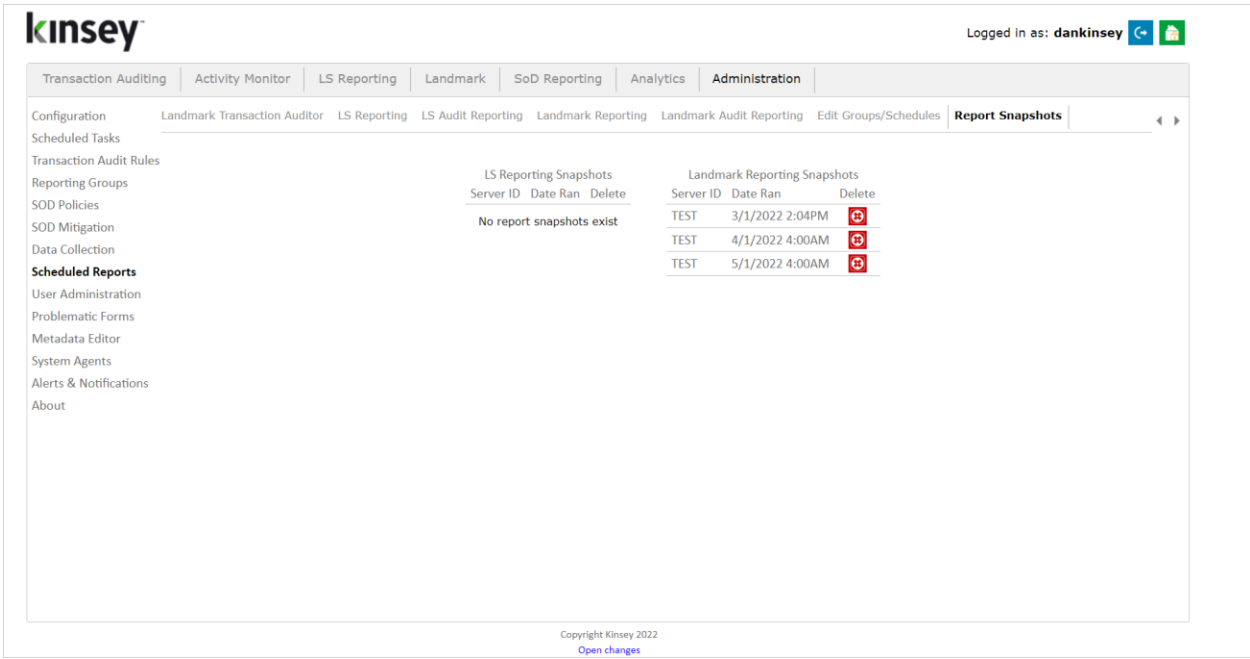




To delete a schedule group select the delete to the right of the schedule.

Report Snapshots

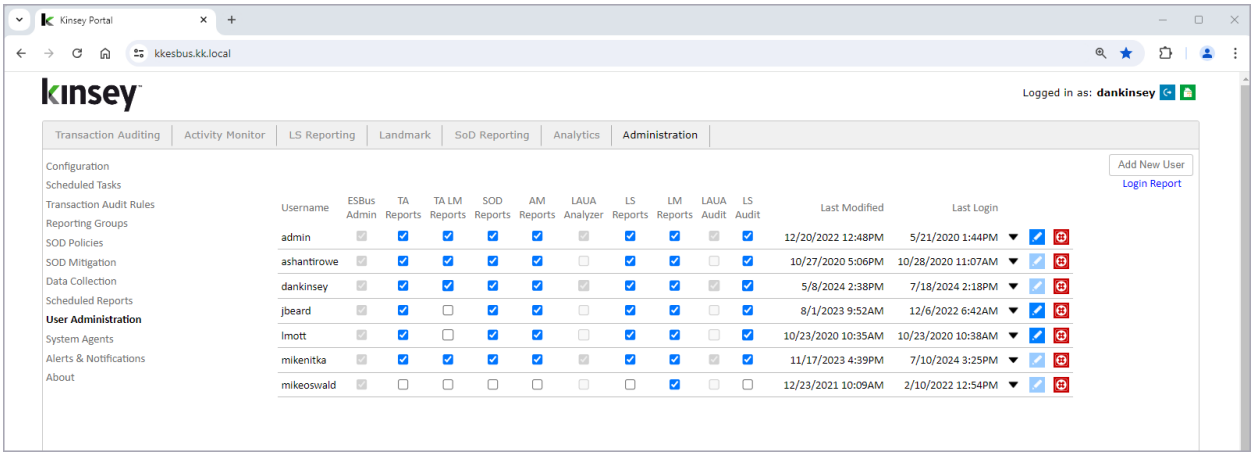
Select the Report Snapshots tab from the Administration > Scheduled Reports link. Snapshots are created through the scheduled task option by either setting up a schedule or manually running the task. A snapshot is a representation of your security settings at any given time. This will allow you to run many of the Security reports to view security as it existing at that time. The snapshot will include all profiles.



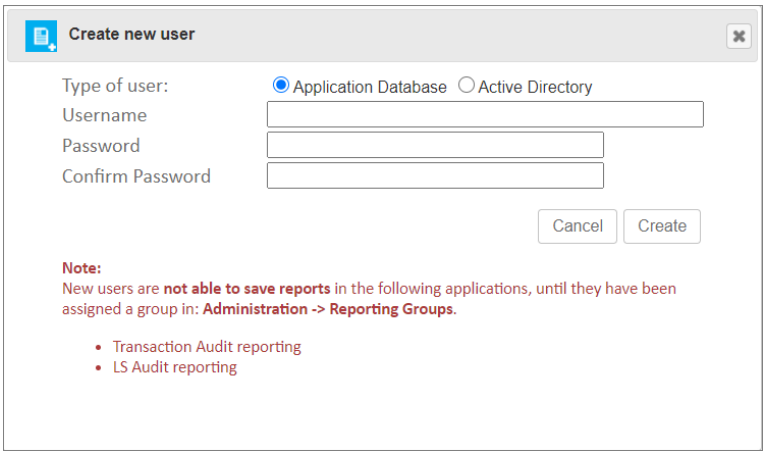
To delete a snapshot select the delete icon next to the desired row.

User Administration

The User Administration page allows you to define new users and assign application security.



To set up a new User select the Add New User button in the upper right corner.



To add new users simply enter the user name and password and select create. By default the user will not have access to any of the applications. Once the user is created you can check the appropriate box to enable an application. If you would like the application to authenticate against Active Directory the user name needs to match their AD account. The password is then maintained in AD.

Note: Active Directory authentication requires a special installation. Please contact us of this is a requirement.

Note: Any user assigned to ESBus Administration will have access to change these settings.

Detailed Application Security Settings

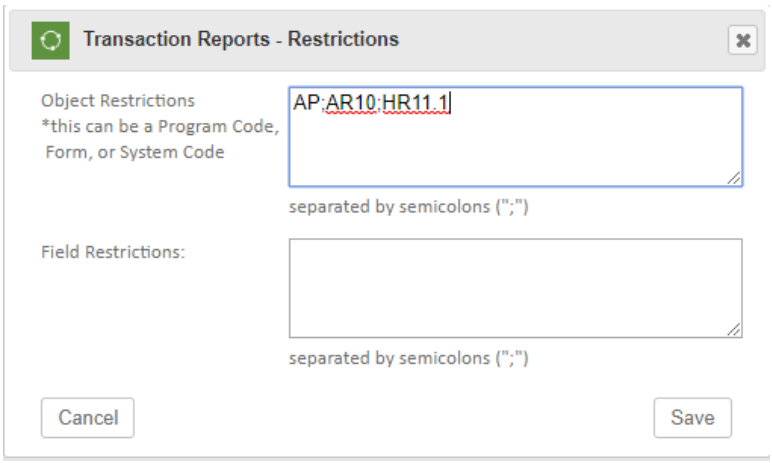
By selecting the dropdown arrow next to the edit icon you can disable or enable specific features within each application.

Report Restrictions (Transaction Audit Reports)

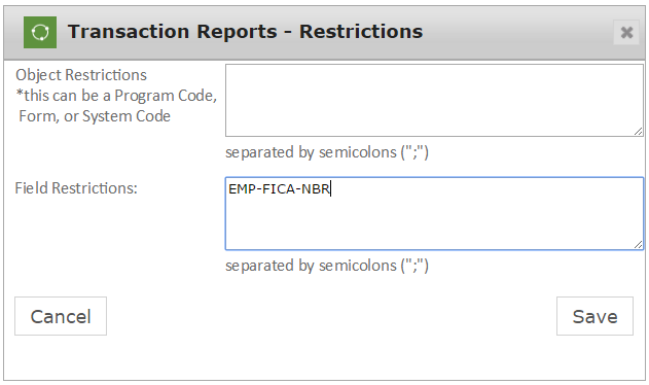
User Report Restrictions allow you to block forms or fields from being displayed in Transaction Auditing reporting, however the data you are restricting still exist in the audit database. The purpose of this feature is to hide information from users you might not want them to see. Since we allow you to create users that may not exist in Lawson this feature adds another layer of security to the data being displayed.

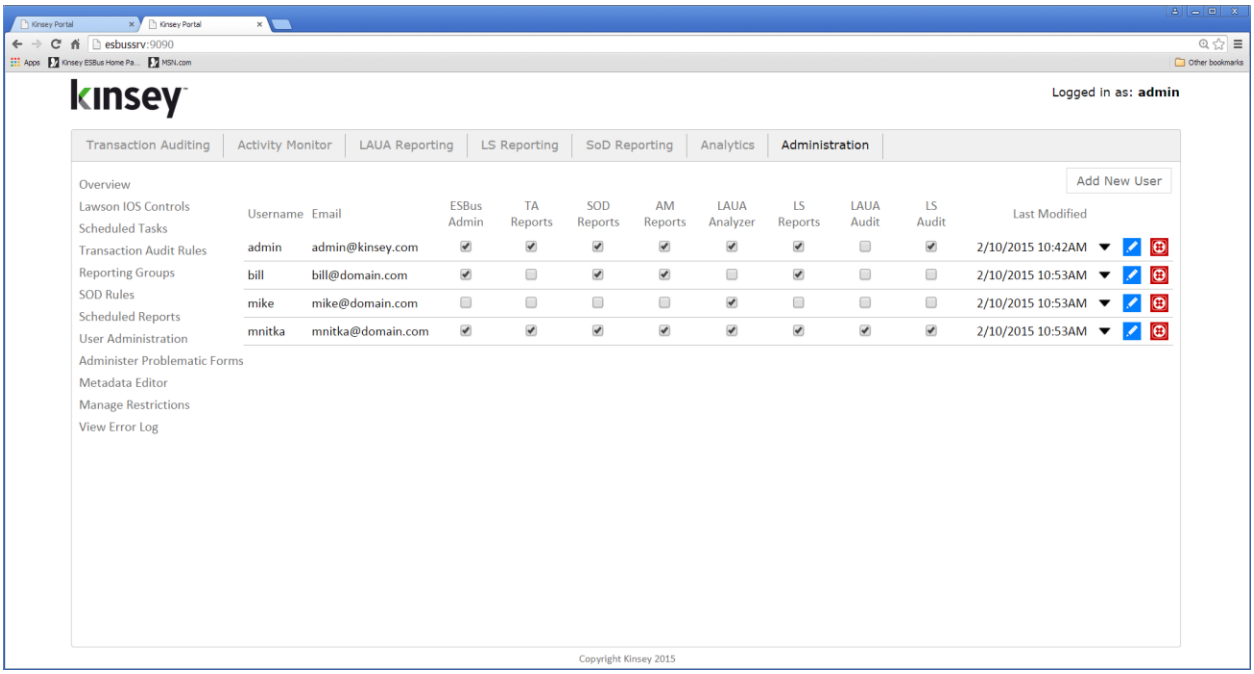
By entering a program code, token (form) ID or system code you can restrict access to view audit data. For example, if you enter HR11 in the object restriction field all audit data from forms HR11.1, HR11.2, HR11.3, etc. will be hidden. The restriction needs to be consistent with Lawson naming conventions. All System Code need to be 2 characters; Programs 4 characters and Tokens (forms) 6 characters.

In this example all AP (System Code) forms; all Customer maintenance (Program AP10) forms (AP10,1, AP10,2, AP10,3) be and form HR11.1 will be blocked.



Additionally you can hide specific field names. In the example below the employees social security report will be removed from all audit reports.



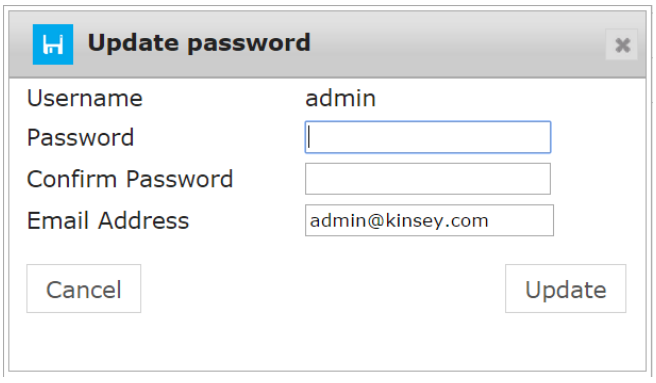


Changing or Deleting a User

To change or delete a user select the appropriate icon to the right of their name.

Note: the email address associate with the user is currently not currently utilized by any of the application.

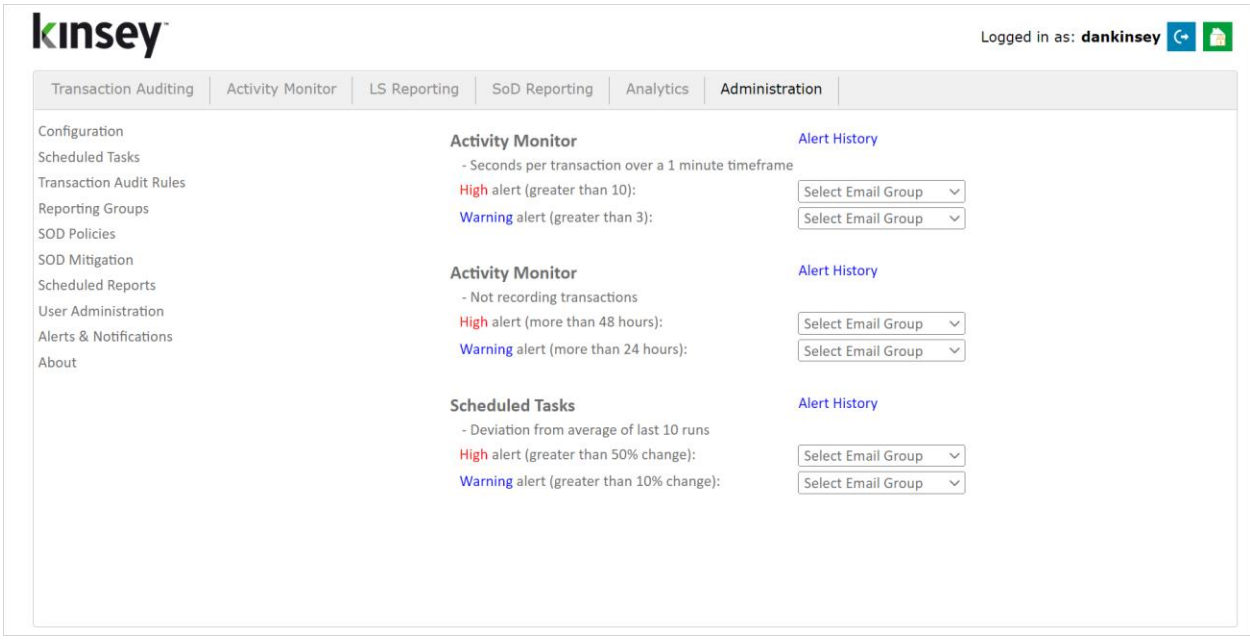
To edit the email address or user password select the edit icon.



Alerts and Notifications

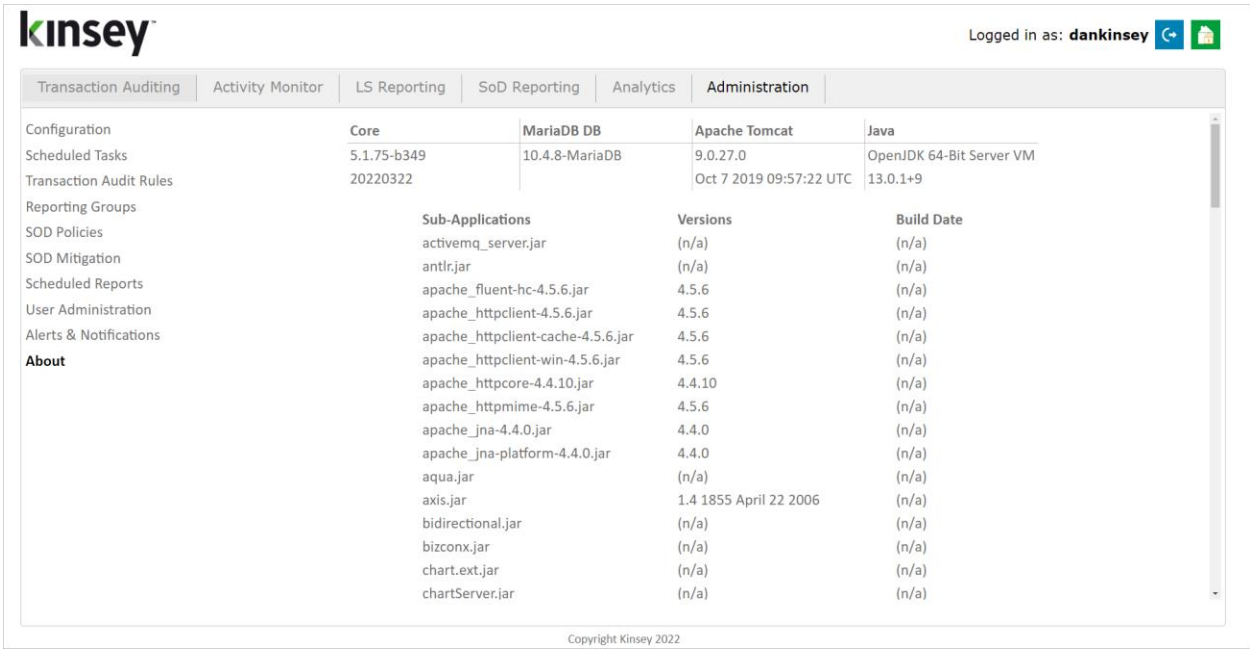
The application can provide notifications if a process has been delayed. This is done my measuring the time since the last successful data collection was performed. If the time frame exceeds the preset parameter an email notification can be sent.

This feature will only work of the server hosting the Kinsey applications is running correctly.



About

The About page will display the versions of your Kinsey applications.



Commonly Asked Questions

Administrative

How do I deactivate the Listener Application or Transaction Auditing?

Refer to Kinsey Summarized WebSphere Installation guide.

When a Kinsey application stops running what is the easiest resolution?

The Kinsey application server can be restarted at any time without affecting the Lawson server or any Lawson process. You should first confirm that the MySQL (or applicable database) and Tomcat processes are running on the Kinsey server and if not manually restart them. Simply rebooting the Kinsey server will accomplish this too. In the majority of cases this will resolve the issue. ***Note: the Kinsey server needs to be running prior to any restart of the Lawson server.***

How to change the ESbus admin user and password?

You can set the Administrator ID through Administration > User Administration by checking the box under the ESBus Admin column.

How do I change the user ESbus User used to access Lawson metadata?

You can set the User ID through Administration > Configuration > Lawson Configuration; Web User and Web Password. There is a configuration option for both the Production and Test environments.

How do I set up new Kinsey application users?

You can find this under the Administration tab, User Administration.

How do I assign a user to a specific reporting group?

You can create and assign groups under the Administration tab; Reporting Groups.

How do I activate a schedule that has been added to a new report?

You can enable or disable schedules through Administration > Scheduled Reports. Select the type of report you need to affect and select the appropriate action.

Segregation of Duties

How do I change the function codes that are used to determine SoD violations?

You can manage the function codes through Administration > Configuration > Segregation of Duties Configuration; SoD Function Code violations.

How do I remove an LS Role from appearing on the LS SoD report?

You can manage the Roles through Administration > Configuration > Segregation of Duties Configuration; Roles to skip with SoD Reporting

How can I enable LS SoD Reporting?

You can activate or deactivate LS9 SoD Reporting through Administration > Configuration > Segregation of Duties Configuration; Security Model LS checkbox

LS Reporting

Where do I change the LDAP user?

You can set the LDAP user through Administration > Configuration > LS Security Configuration (Production or Test); LDAP User.

Where do I change the LDAP password?

You can set the LDAP password through Administration > Configuration > LS Security Configuration (Production or Test); LDAP Password.

Where do I change the LDAP default profile for reporting?

You can set the default profile through Administration > Configuration > LS Security Configuration (Production or Test); LDAP Profile.

Why don't I see my changes to Lawson or Landmark security in the Reports?

The dashboard collects the data from the security databases on a nightly schedule. Changes made during the day will not be included in the reports until the collection process is run either via the scheduled time or on demand. You can manually run the process through Administration > Scheduled Tasks > LS LDAP data collection or Landmark Security data collection for either the Production or Test environments.

Why don't I see my changes to security on the Security Audit Report?

The security report collects the data from Infor's audit tables on a nightly schedule. Changes made during the day will not be included in the reports until the collection process is run via the scheduled time or on demand. You can manually run the process through the Administration > Scheduled Tasks > Collect LS Auditing data (using ERP HTTP Call) or Landmark Transaction data collection for either the Production or Test environments.

Why am I missing data on the LS Security Reports?

This more than likely has to do with a parameter setting in LDAP. See *LS Reporting Data Collection Problems* below to resolve this issue.

Activity Monitor (Listener)

How can I tell if the S3 Listener is running?

You can view activity counts for the past 24 hours on the dashboard Analytics page for Production and Test server. Note that the graphs reflect combined activity for both environments. To verify Prod version Test use the Listener detail activity report on the LS Security Reporting dashboard.

You can also select an email group on the Alerts and Notifications page to notify you if Activity Monitor is not working correctly.

How can I set the data retention policy for Listener activity?

You can set the Listener retention policy through Administration > Configuration > Lawson Configuration (Production or Test); field *Listener Data Retention Time*.

Problem Resolution

Kinsey recommends the installation of a virtual server (VM) to host the Kinsey applications, Tomcat, Java and a MySQL (or MariaDB) database. The database contains 3 types of tables; system parameters, Lawson metadata and client data. The system parameters are required for Kinsey's WebSphere application. That application will send transactions from the Lawson server to the VM. This is only the case for customers running Transaction Auditing, Activity Monitor (Listener) for the S3 applications.

The Lawson metadata is used strictly for Kinsey reports. This includes information like form names and function code descriptions. This data is collected on the initial installation of the application and can be refreshed manually when Lawson applications are updated.

Depending on the applications purchased, the client data can consist of anything from transaction level data to LDAP security settings. However, unless you are running Kinsey's Transaction Auditing application, Lawson application field level data will never be collected. Security (LDAP) data is collected via a scheduled process that generally runs every night. You can also run the processes manually as needed.

Transaction Auditing and Activity Monitor (Listener) data is collected real time. There is no scheduled task for these processes.

Virtual Server System Settings

1. JVM Memory (relates to SoD Reporting only)
    - This setting depends on how much memory has been allocated to the virtual server and whether the server is running Windows or Linux. For a Windows OS JVM cannot be set to use more than ½ the memory available, for Linux its variable.
2. Kinsey VM Memory (8 MB min)
    - This is a minimum requirement and can vary greatly depending on the OS and the size of the customer's security model. We will always recommend more memory for a Windows server than for a Linux server.
3. If LDAP Paging is used by Lawson
    - ADAM and Tivoli page sizes are based on how Lawson is set. Kinsey does not make a change to these settings.
4. If LDAP is not used by Lawson
    - If using Tivoli then the maximum records has to be set to (Users x Identities available).

Potential Lawson Issues

(1) Portal screens aren't responding.

Applies to: Transaction Auditing, Activity Monitor (Listener)

It's critical that the Kinsey VM is fully operational prior to starting Lawson. More specifically, Tomcat and MySQL must be running on the VM. Kinsey's WebSphere application will try to connect to the Kinsey VM and retrieve configuration settings stored in MySQL (or MariaDB). If a connection cannot be made, Lawson's Portal application will not respond correctly.

Note: The Kinsey VM can be restarted anytime without stopping Lawson. When the Kinsey VM is offline you will not be able to collect data from the Lawson server for reporting purposes, but it will not impact Lawson. See the "WebSphere Hangs" section below for exception to this note.

Corrective Steps.

Restart Lawson after each step until Lawson Portal is responding

1. Make sure the Kinsey VM is running, if not start the Kinsey VM and validate that you can access the Kinsey portal page.
2. Restart MySQL (or MariaDB) and Tomcat on the VM in that sequence and validate that you can access the Kinsey portal page..
3. If Lawson still won't start then reboot the VM and validate that you can access the Kinsey portal page.
4. If Lawson still won't start then deactivate Listener (refer to page 9 of Kinsey Active MQ Summarized Installation Guide)

If Listener needs to be deactivated please schedule time with Kinsey to evaluate the condition of the VM prior to reactivating the application. Possible problems include hardware failure, network configuration changes (i.e. Lawson or application server IP address changes), MySQL corruption, hard drive is full or JAVA update has changed settings.

(2) WebSphere hangs

Applies to: Transaction Auditing, Activity Monitor (Listener)

The Kinsey application uses the JMS queues to collect and send data to the Kinsey VM. If the Kinsey VM is unable to received messages for any reason the JMS queues will hold the transactions until the Kinsey VM is back online. This is similar to an email message being stuck in an outbox. If the Kinsey VM is left off-line for an extended period of time the JMS queues can fill up and potentially fill up the hard drive where the WebSphere system logs are kept. By default the WebSphere JMS queues will store 500MB of

data per node. Kinsey does not change this setting. For instance, if you have 5 nodes on your system you need to make sure you have at least 2.5GB of available hard drive space on the same drive where the WebSphere logs are kept.

Provided you have sufficient room on the drive and the 500MB limit is reached the JMS queue will stop accepting new messages (listener data). This will not cause the system to crash but these transactions will be lost. Once the Kinsey VM is back online all of the messages (transactions) will be sent to the VM.

Corrective Steps:

1. Validate that you have enough room on your log drive to hold 500MB x # of nodes.
2. Manually purge the JMS queue and restart WebSphere

Virtual Server Monitoring

This is a list of items that could/should be monitored on the Kinsey server:

PORT CHECK:

MySQL – Port 3306

Should return something similar to:

J5.6.20t>♥%h`*K{M ☻ Ç§#_75D6"FwG=<mysql_native_password

TOMCAT – Port 80

(This will not return anything for a GOOD)

SERVICE CHECK (if possible):

MySQL - (service mysqld status) OR (ps -ef | grep mysql)

Tomcat - (ps -ef | grep tomcat)

PING: Kinsey Server (for network connection check)

LS Reporting Data Collection Problems

Data missing from LS Security Reports

The Kinsey application requires specific parameters to be set in order to ensure that all data is collected properly. If you are experiencing problems where the reports only show a partial list of Users, Roles or Security Class you need to confirm that your IBMSLAPD size is set to unlimited.

If you are see no security data on the Kinsey reports that usually indicates that the LDAP or Landmark credentials used by the Kinsey application have been changed. Confirm that the password for the Kinsey account has not been changed.

Notes: