kinsey™

Administrator Guide

Document containing administration instructions related to Transaction Auditing, Activity Monitor, Segregation of Duties, LAUA Reporting, LS9 Reporting and Security Auditing

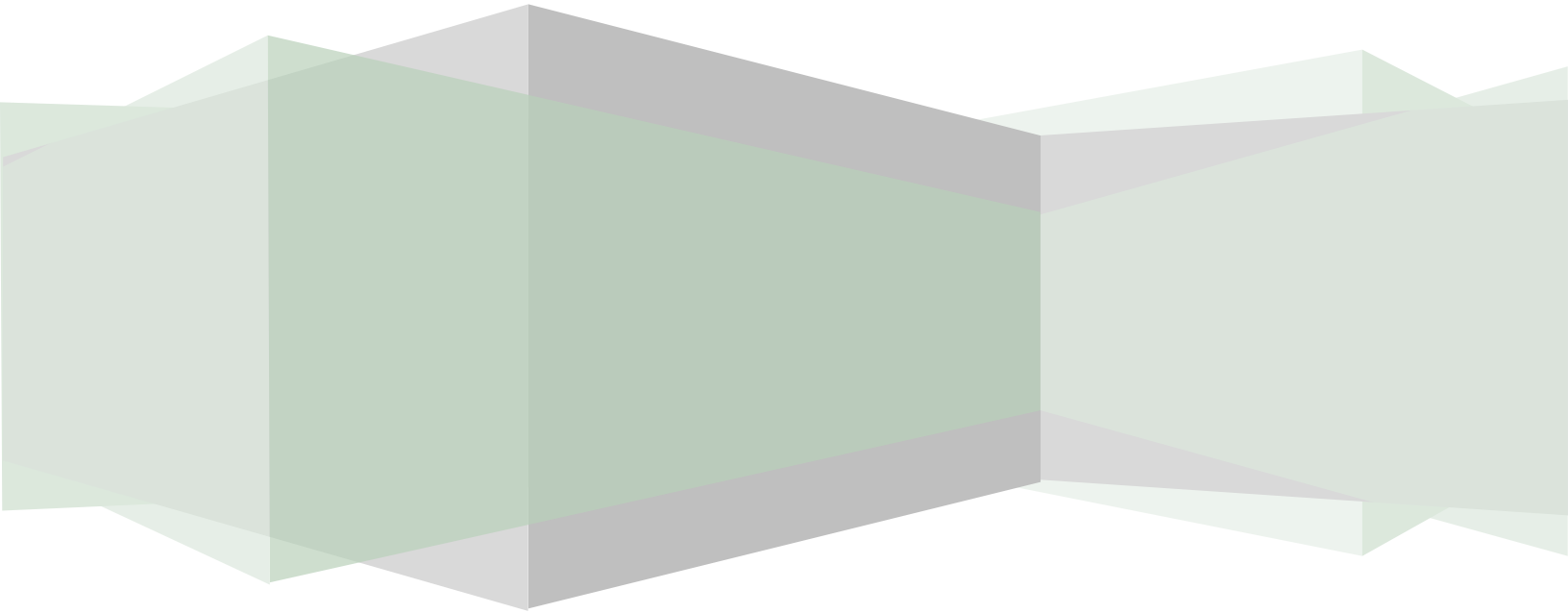
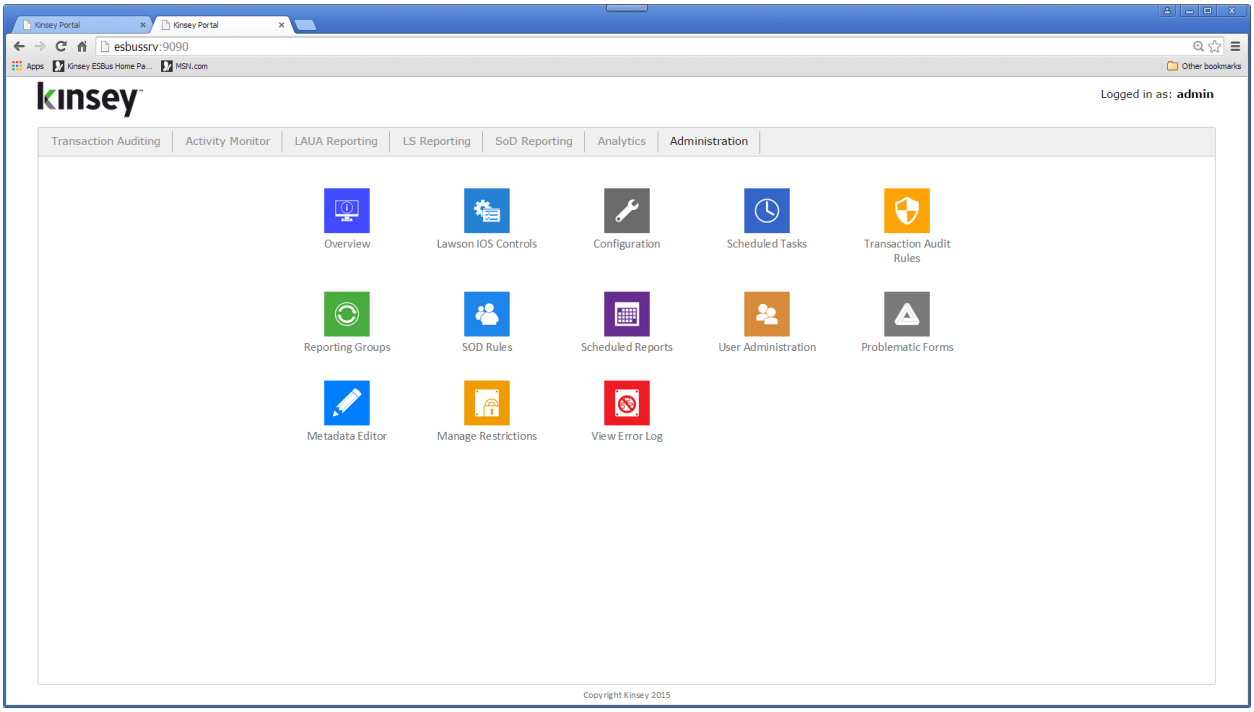


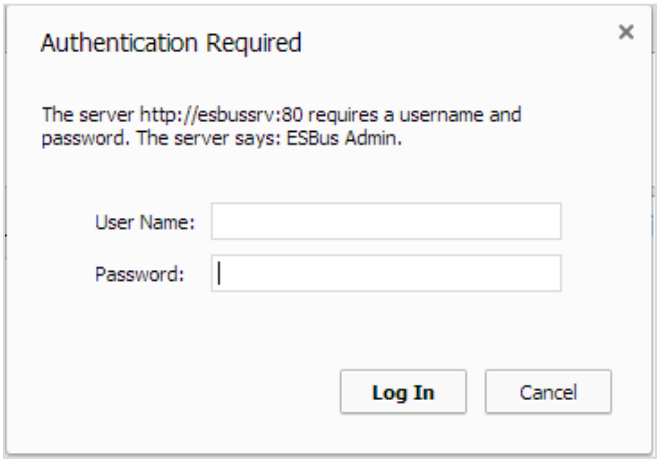
Table of Contents

Administrative Login

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



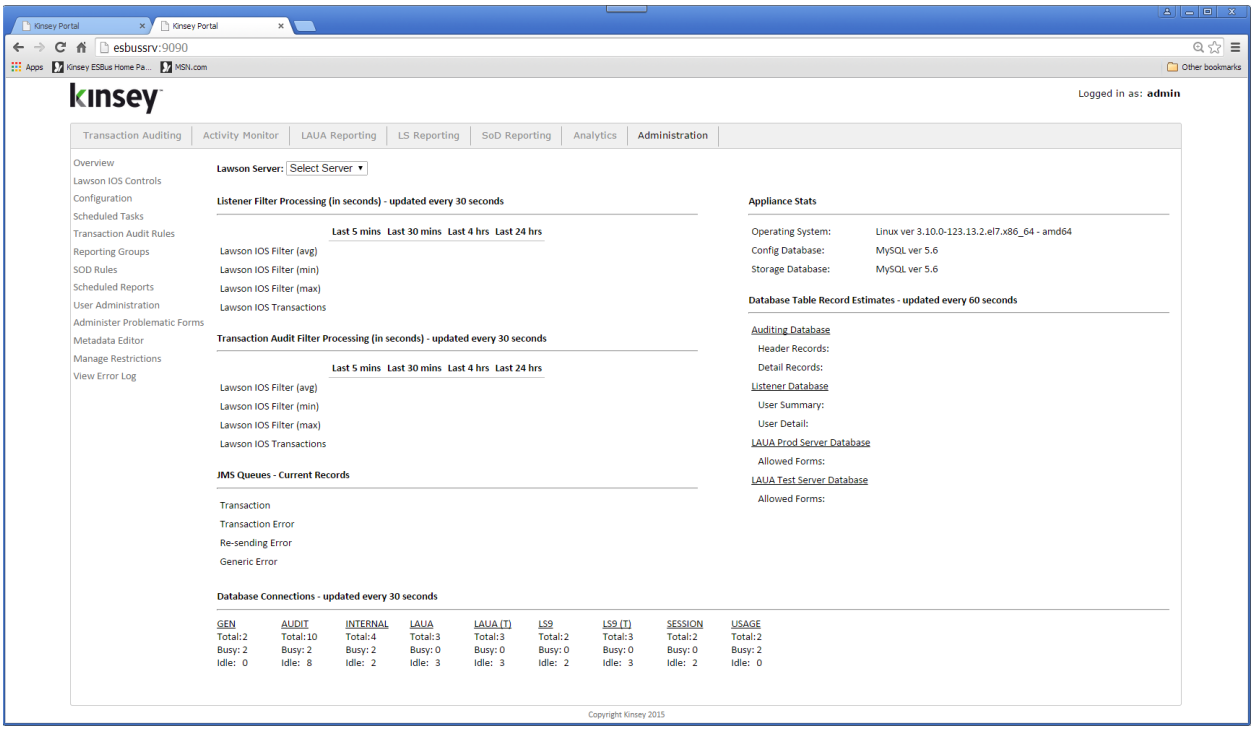
Select the Administration tab to log into the Admin page



Enter your administrative User name and Password

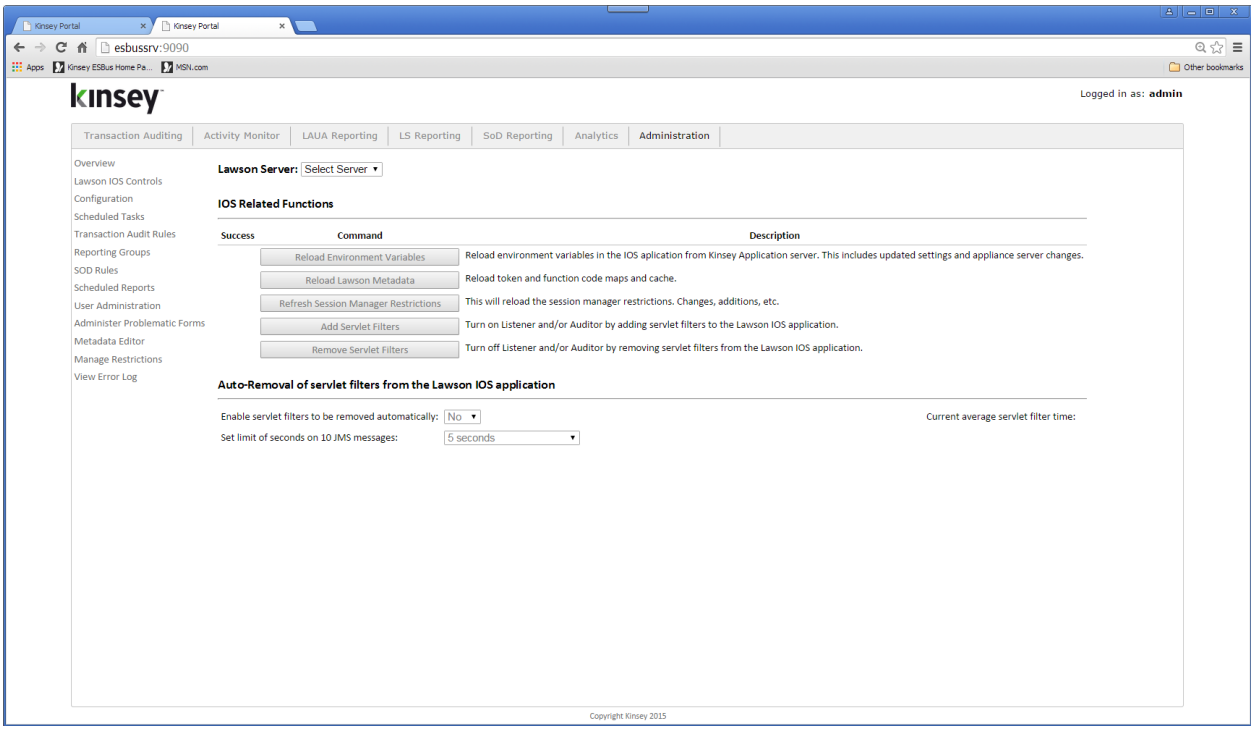
Overview

The overview option provides statistical information regarding the collection of Transaction Auditing and Activity Monitor data.



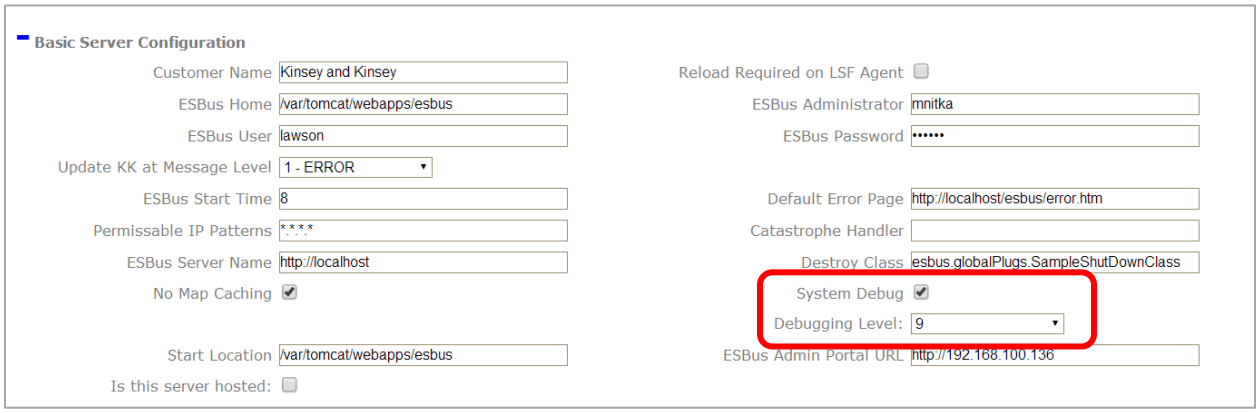
Lawson IOS Controls

The Lawson IOS Control form is not used by the current release of the application. The manual options on this screen are now automated. The form is only required for customers running Kinsey auditing and listening versions prior to 2009.



Configuration

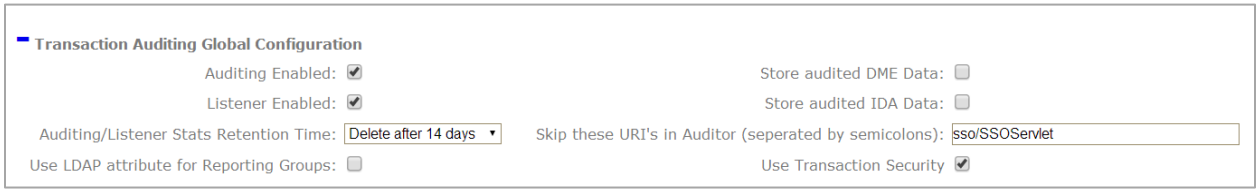
Basic Server Configuration



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.

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

Use LDAP Attribute

Store DME Data

Store IDA Data

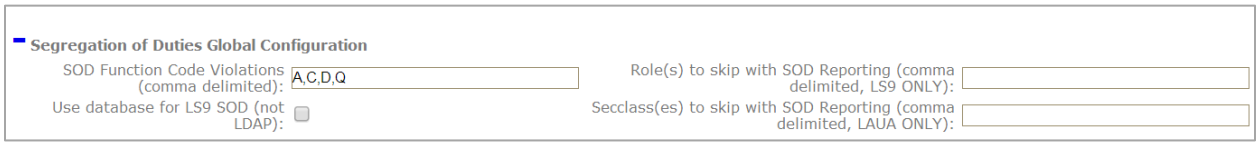
Skip URI's

Use TA Security

Use LDAP Attribute for Reporting Groups

Segregation of Duties Global Configuration

This option is only needed for customers who have purchased the Segregation of Duties application.



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 or LAUA security class 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 LS9 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.

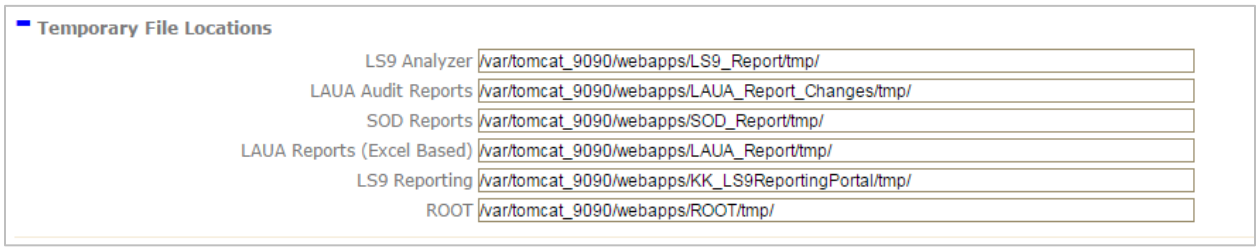
Use database for LS SOD (not LDAP) – Check this option if you want the SOD reports to use the Kinsey LS SQl database to check for SOD violations or leave this option unchecked to if you want SOD to check LDAP directly.

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, D and Q are default settings. The actual function codes used by the SOD application are defined in the SOD Function Code Violations field.

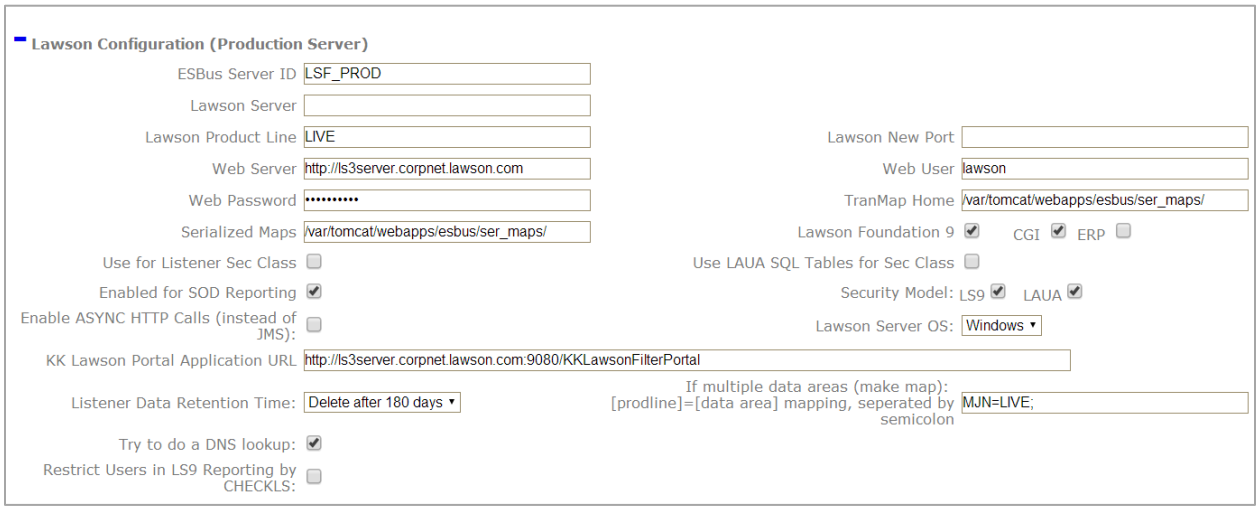
Temporary File Locations

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.



Lawson Configuration Production Server

This information will be configured on installation.

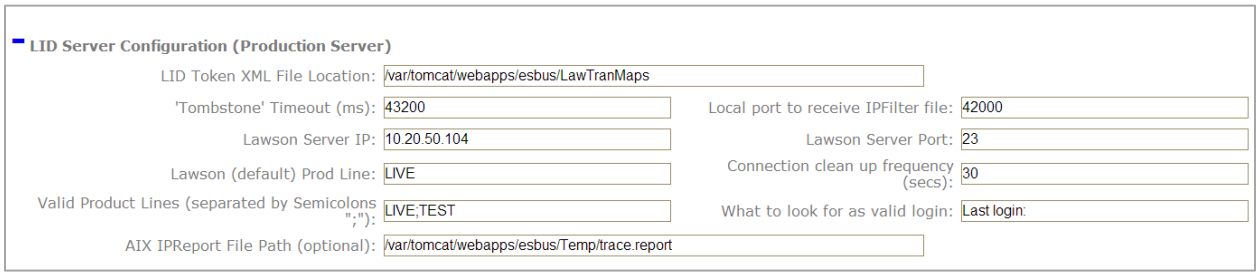


The follow fields may occastionally need to be updated

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.

LID Server Configuration (Production Server)

This information will be configured on installation. For questions please contact Kinsey technical support.

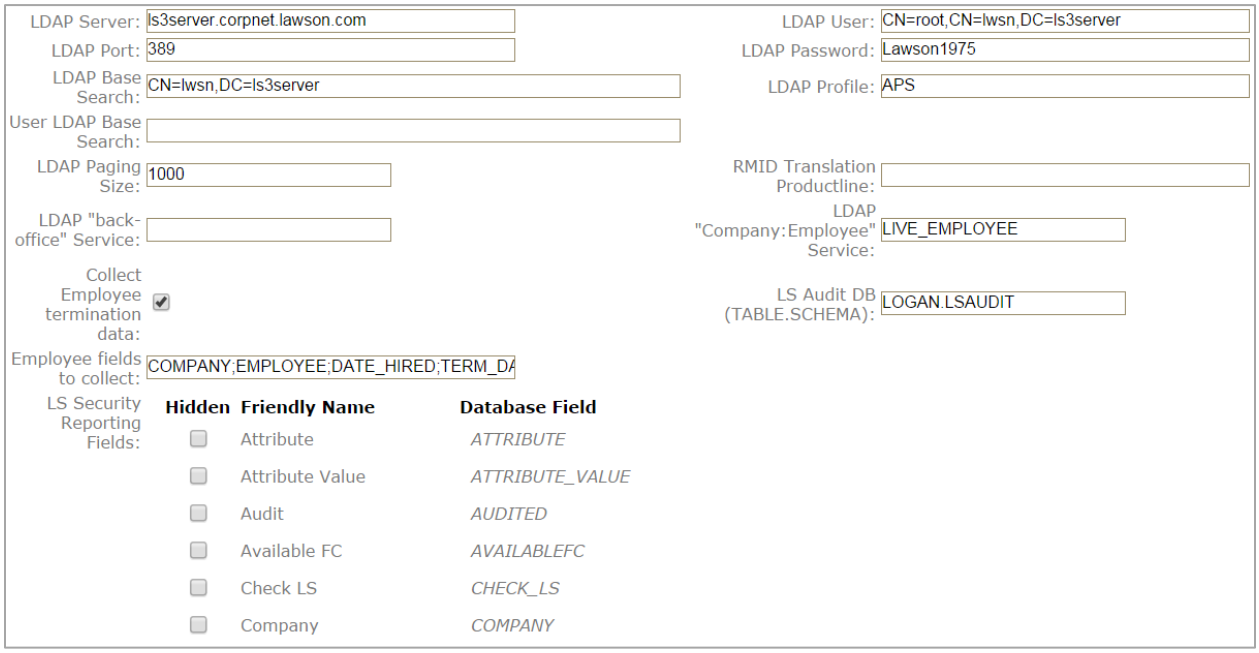


ESS Tracking Application Configuration (Production Server)

This form is currently not in use.

LS9 Security Configuration (Production Server)

This information will be configured on installation.



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 the report is run.

Lawson Configuration Test Server

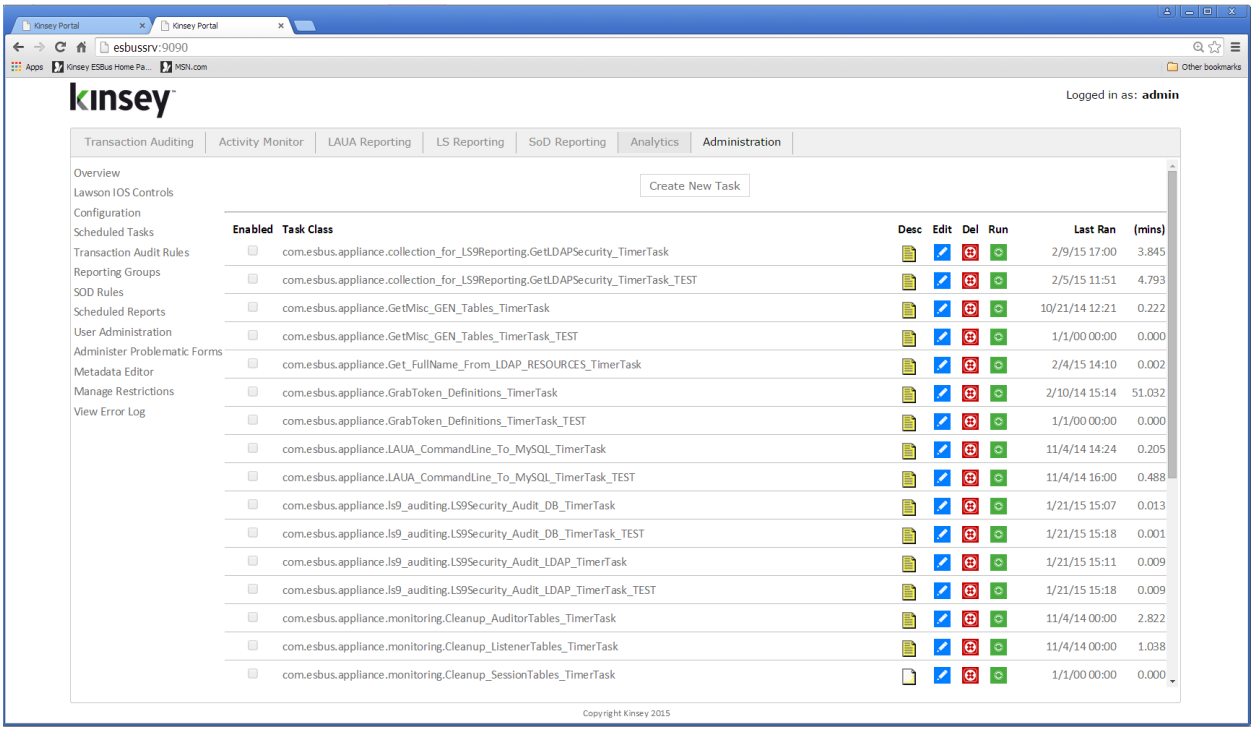
Refer to the Lawson Configuration Production Server instructions for more information.

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 programs that will retrieve or purge data for the reporting databases.



Applications: LS Reporting
Purpose: Creates a point in time snap shot of LS security data for the PRODUCTION environment
Schedule: As Scheduled
Task:
com.esbus.appliance.collection_for_LS9Reporting.GetLDAPSecurity_Snapshot_TimerTask

Applications: LS Reporting
Purpose: Creates a point in time snap shot of LS security data for the TEST environment
Schedule: As Scheduled
Task:
com.esbus.appliance.collection_for_LS9Reporting.GetLDAPSecurity_Snapshot_TimerTask_TEST

Applications: LS Reporting
Purpose: Collects LS security data for the PRODUCTION environment
Schedule: Nightly
Task: **com.esbus.appliance.collection_for_LS9Reporting.GetLDAPSecurity_TimerTask**

Applications: LS Reporting
Purpose: Collects LS security data for TEST environment
Schedule: Nightly
Task:**com.esbus.appliance.collection_for_LS9Reporting.GetLDAPSecurity_TimerTask_TEST**

Applications: LS Reporting, LS Analyzer
Purpose: Collects all LS User Fullnames (Last name, first name, username)
Schedule: Nightly
Task: **com.esbus.appliance.Get_FullName_From_LDAP_RESOURCES_TimerTask**

Applications: LAUA Analyzer, LAUA Auditor, Activity Monitor, LS Reporting
Purpose: LAUA data collection (PROD)
Schedule: Nightly
Task: **com.esbus.appliance.LAUA_CommandLine_To_MySQL_TimerTask**

Applications: LAUA Analyzer, LAUA Auditor, Activity Monitor, LS Reporting
Purpose: LAUA data collection (TEST)
Schedule: Every 4 hours
Task: **com.esbus.appliance.LAUA_CommandLine_To_MySQL_TimerTask_TEST**

Applications: LS Auditing
Purpose: LS Audit data collection (TEST) - uses Logan Database option
Schedule: Every 15 minutes
Task: **com.esbus.appliance.ls9_auditing.LS9Security_Audit_DB_TimerTask_TEST**

Applications: LS Auditing
Purpose: LS Audit data collection (PROD) – uses LDAP option in Lawson
Schedule: Every 15 minutes
Task: **com.esbus.appliance.ls9_auditing.LS9Security_Audit_LDAP_TimerTask**

Applications: Transaction Auditing
Purpose: Clean up TA Tables based on the audit rule retention policy defined
Schedule: Nightly
Task: **com.esbus.appliance.monitoring.Cleanup_AuditorTables_TimerTask**

Applications: Activity Monitor – Listener Activity
Purpose: Clean up Listener Tables
Schedule: Nightly
Task: **com.esbus.appliance.monitoring.Cleanup_ListenerTables_TimerTask**

Applications: Transaction Auditing and Activity Monitor (Listener) Table Statistics
Purpose: Clean up TA adn AM statistic tables
Schedule: Nightly
Task: **com.esbus.appliance.monitoring.Cleanup_TAStatsTables_TimerTask**

Applications: LAUA Reporting, Activity Monitor, Transaction Auditor
Purpose: Gets Windows NTID translations (PROD) (listusermap.exe MUST be copied to cgi-bin folder on Lawson Portal - to work correctly)
Schedule: Nightly
Task: **com.esbus.appliance.serverUtil.GetLawsonListuserMap_TimerTask**

Applications: LAUA Reporting, Activity Monitor, Transaction Auditor
Purpose: Gets Windows NTID translations (TEST) (listusermap.exe MUST be copied to cgi-bin folder on Lawson Portal - to work correctly)
Schedule: Nightly
Task: **com.esbus.appliance.serverUtil.GetLawsonListuserMap_TimerTask_TEST**

Applications: Dashboard
Purpose: Runs SOD Reporting for system - this creates data for dashboard graph
Schedule: Nightly
Task: **com.esbus.appliance.SOD_PolicyCheck_SystemRun_TimerTask**

Applications: LS Analyzer
Purpose: Collects LS data (PROD)
Schedule: Nightly
Task: **com.esbus.LS9Report.LS9Analyzer_LDAPDataCollection_TimerTask**

Applications: LS Analyzer
Purpose: Collects LS data (TEST)
Schedule: Nightly
Task: **com.esbus.LS9Report.LS9Analyzer_LDAPDataCollection_TimerTask_TEST**

Applications: All Reporting Applications
Purpose: Collects GEN - Tokens, Tables, Category metadata (PROD)
Schedule: Typically only run on server install or when token are added to the system
Task: **com.esbus.appliance.GetMisc_GEN_Tables_TimerTask**

Applications: All Reporting Applications
Purpose: Collects GEN - Tokens, Tables, Category metadata (TEST)
Schedule: Typically only run on server install or when token are added to the system
Task: **com.esbus.appliance.GetMisc_GEN_Tables_TimerTask_TEST**

Applications: All Reporting Applications
Purpose: Collects GEN - Tokens definitions (formdef.exe) (PROD)
Schedule: Typically only run on server install or when token are added to the system
Task: **com.esbus.appliance.GrabToken_Definitions_TimerTask**

Applications: All Reporting Applications
Purpose: Collect GEN - Tokens definitions (formdef.exe) (TEST)
Schedule: Typically only run on server install or when token are added to the system
Task: **com.esbus.appliance.GrabToken_Definitions_TimerTask_TEST**

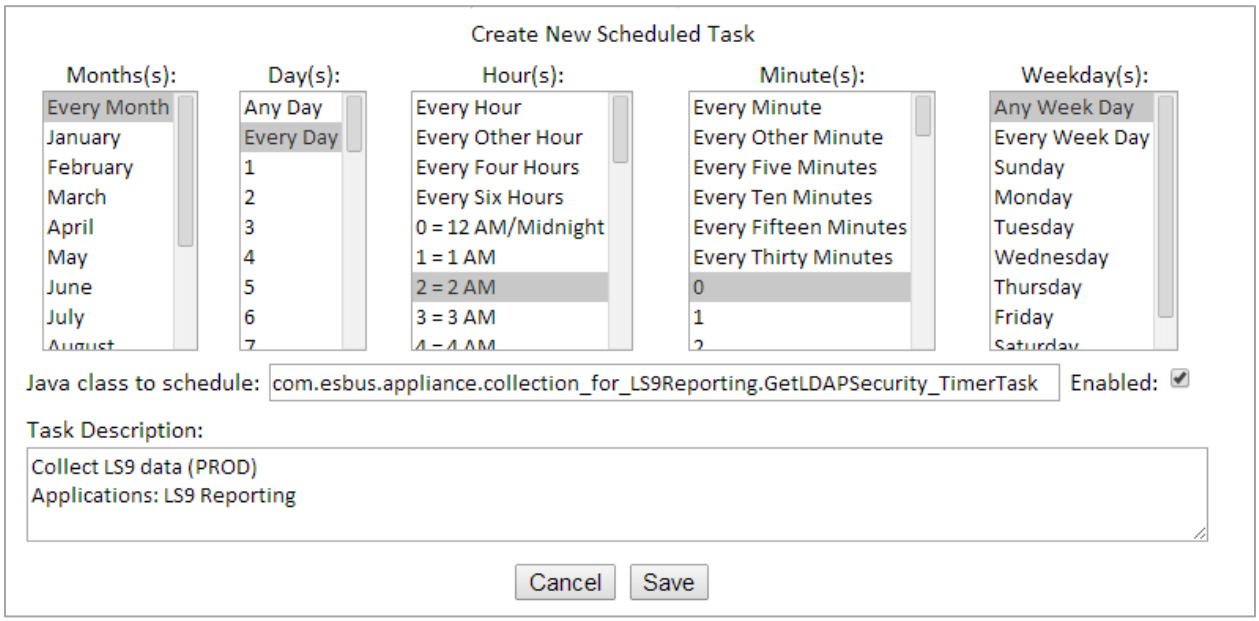
Applications: LS Auditing
Purpose: LS9 Audit data collection (PROD) - uses Logan Database option
Schedule: Nightly
Task: **com.esbus.appliance.ls9_auditing.LS9Security_Audit_DB_TimerTask**

Applications: LS Auditing
Purpose: LS Audit data collection (TEST) – uses LDAP option in Lawson
Schedule: Nightly
Task: **com.esbus.appliance.ls9_auditing.LS9Security_Audit_LDAP_TimerTask_TEST**

Applications: Landmark Security Reporting
Purpose: Collects Landmark security data for the PRODUCTION environment
Schedule: Nightly
Task: com.esbus.appliance.collection_for_LMReporting.GetLMSecurity_TimerTask

Applications: Landmark Security Reporting
Purpose: Collects Landmark security data for the TEST environment
Schedule: Nightly
Task: com.esbus.appliance.collection_for_LMReporting.GetLMSecurity_TimerTask_TEST

Defining a Schedule



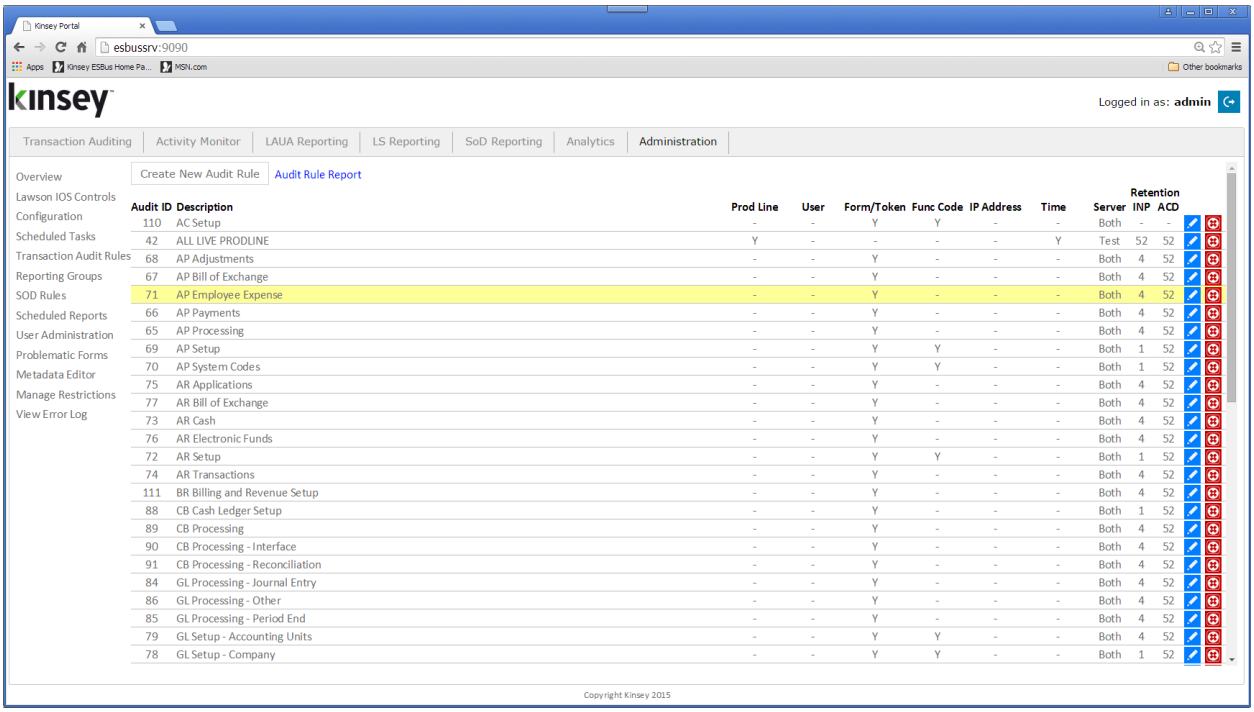
Select the Edit icon next to the process you want to schedule.

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'

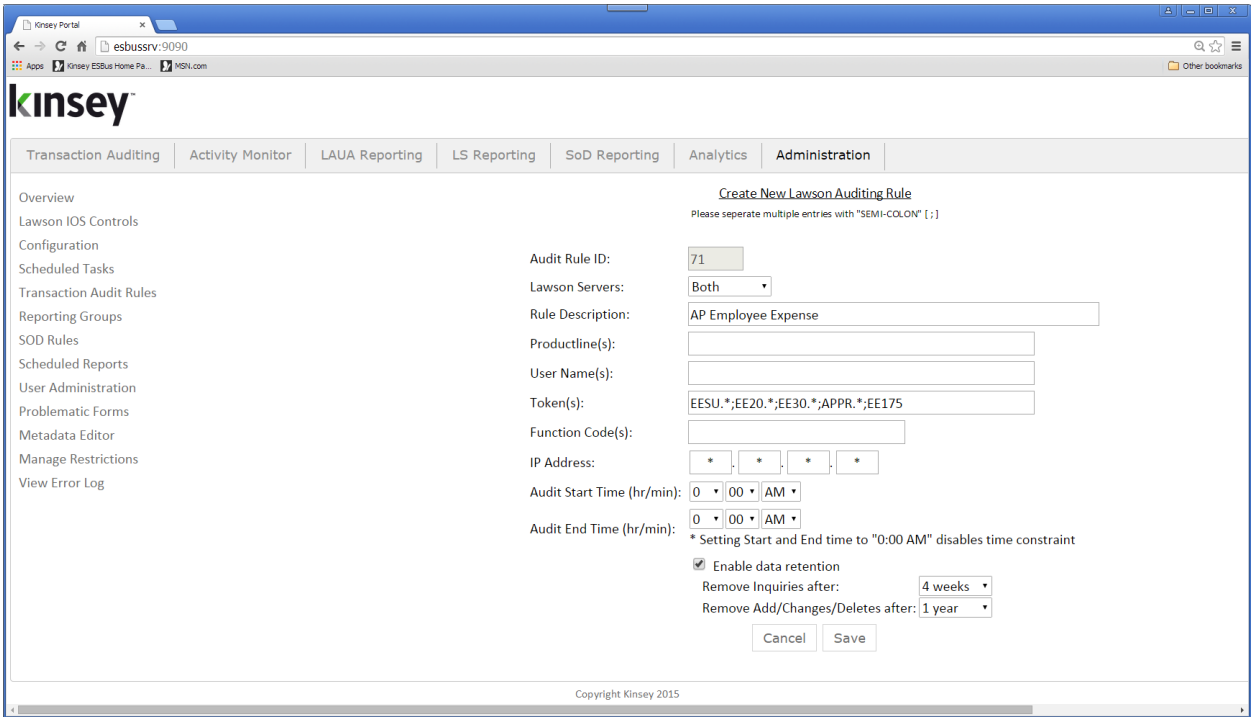
Transaction Audit Rules

From the Adminstrative page select ”Transaction Audit Rules”. The existing rules will be displayed. 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” button.



Audit ID	Description	Prod Line	User	Form/Token	Func Code	IP Address	Time	Server	Retention INP	Retention ACD
110	AC Setup	-	-	Y	Y	-	-	Both	-	-
42	ALL LIVE PRODLINE	Y	-	-	-	-	Y	Test	52	52
68	AP Adjustments	-	-	Y	-	-	-	Both	4	52
67	AP Bill of Exchange	-	-	Y	-	-	-	Both	4	52
71	AP Employee Expense	-	-	Y	-	-	-	Both	4	52
66	AP Payments	-	-	Y	-	-	-	Both	4	52
65	AP Processing	-	-	Y	-	-	-	Both	4	52
69	AP Setup	-	-	Y	Y	-	-	Both	1	52
70	AP System Codes	-	-	Y	Y	-	-	Both	1	52
75	AR Applications	-	-	Y	-	-	-	Both	4	52
77	AR Bill of Exchange	-	-	Y	-	-	-	Both	4	52
73	AR Cash	-	-	Y	-	-	-	Both	4	52
76	AR Electronic Funds	-	-	Y	-	-	-	Both	4	52
72	AR Setup	-	-	Y	Y	-	-	Both	1	52
74	AR Transactions	-	-	Y	-	-	-	Both	4	52
111	BR Billing and Revenue Setup	-	-	Y	-	-	-	Both	4	52
88	CB Cash Ledger Setup	-	-	Y	-	-	-	Both	1	52
89	CB Processing	-	-	Y	-	-	-	Both	4	52
90	CB Processing - Interface	-	-	Y	-	-	-	Both	4	52
91	CB Processing - Reconciliation	-	-	Y	-	-	-	Both	4	52
84	GL Processing - Journal Entry	-	-	Y	-	-	-	Both	4	52
86	GL Processing - Other	-	-	Y	-	-	-	Both	4	52
85	GL Processing - Period End	-	-	Y	-	-	-	Both	4	52
79	GL Setup - Accounting Units	-	-	Y	Y	-	-	Both	4	52
78	GL Setup - Company	-	-	Y	Y	-	-	Both	1	52

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.



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.

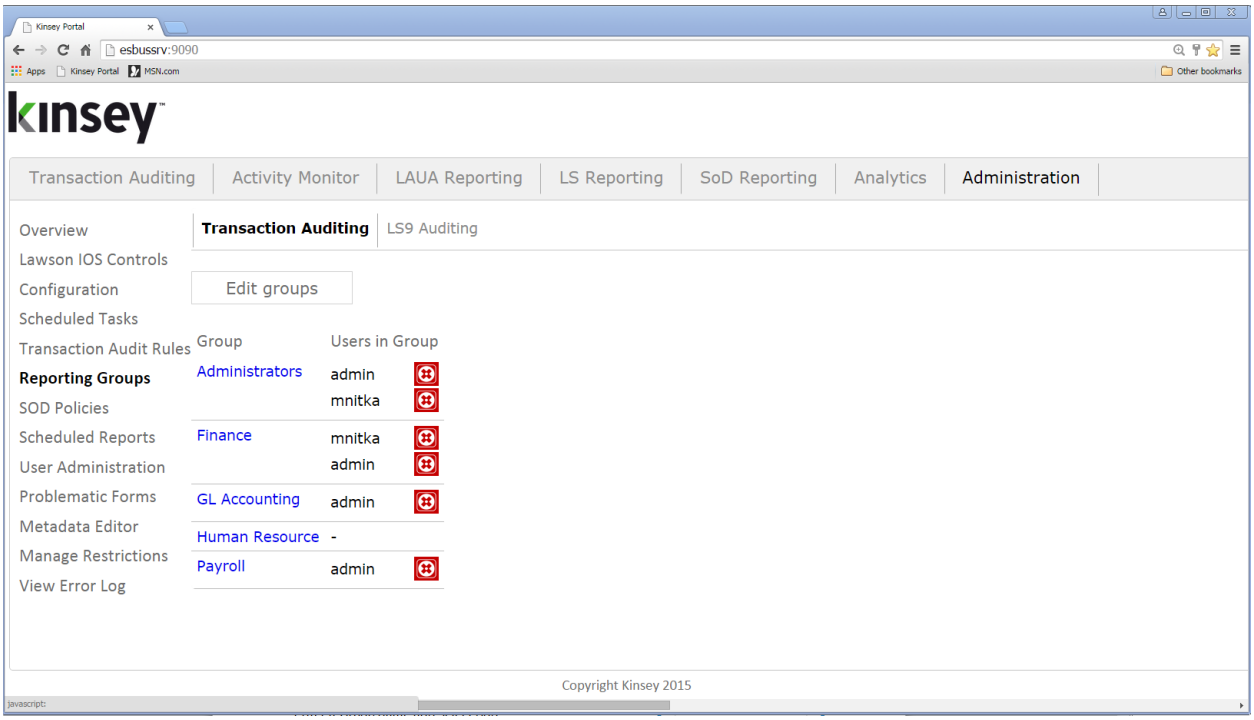
Remove Add/Change/Deletes after:

Enter the time period that you want to keep all non-inquire records.

Select **SAVE** to save your entry.

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.



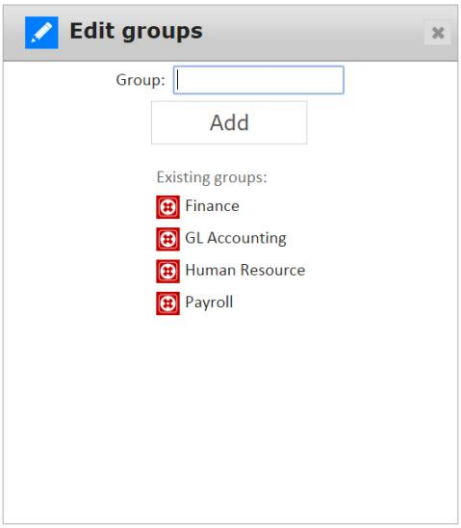
Select Reporting Groups from the left navigation pane. All users previously created under User Administration will be display.

Creating or Deleting a New Group

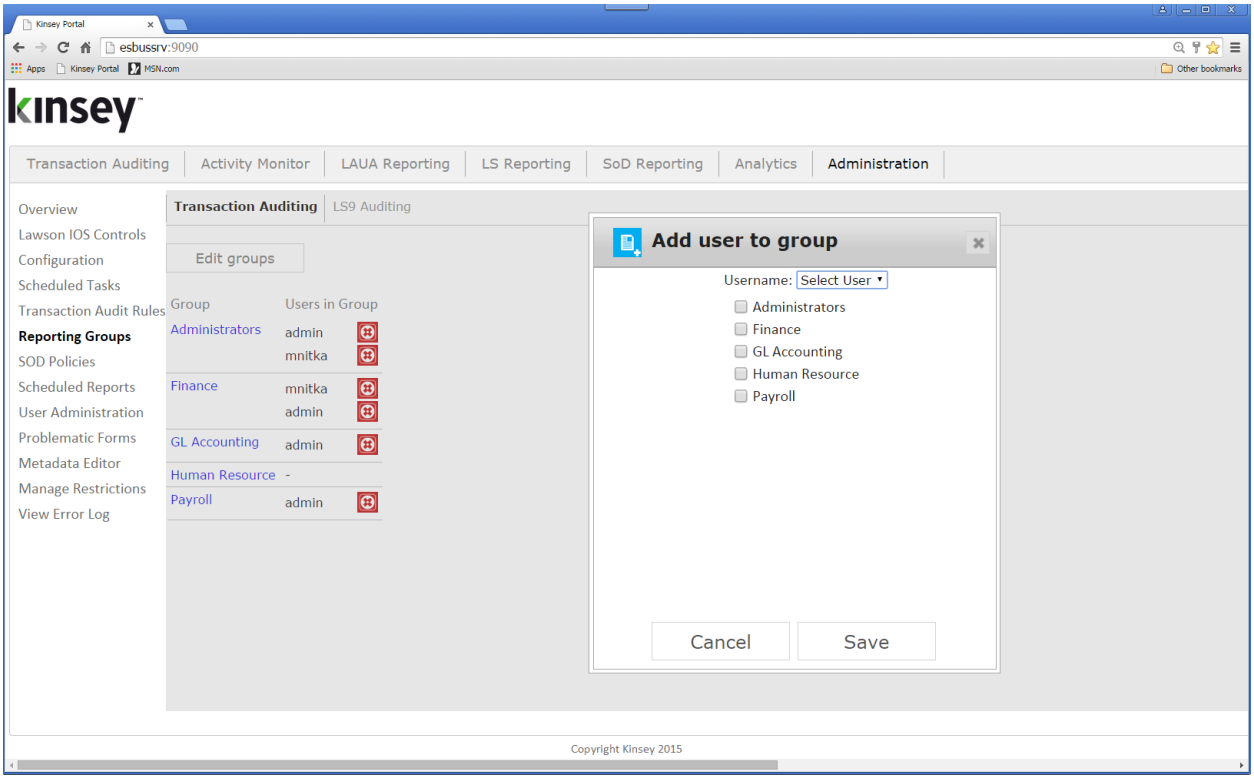
To create new groups click on the Edit Group button.

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

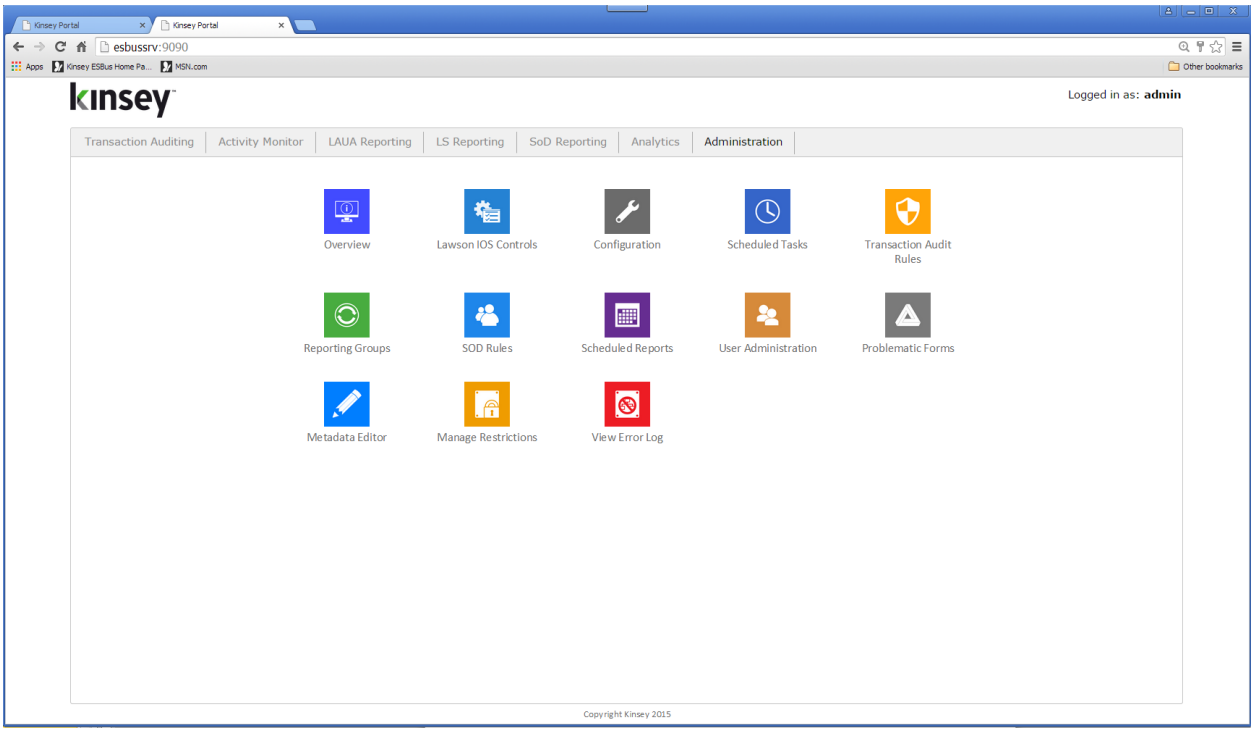


Click on any of the Group names the add a user to the group. To delete a user select the delete icon next to the user's name.

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.

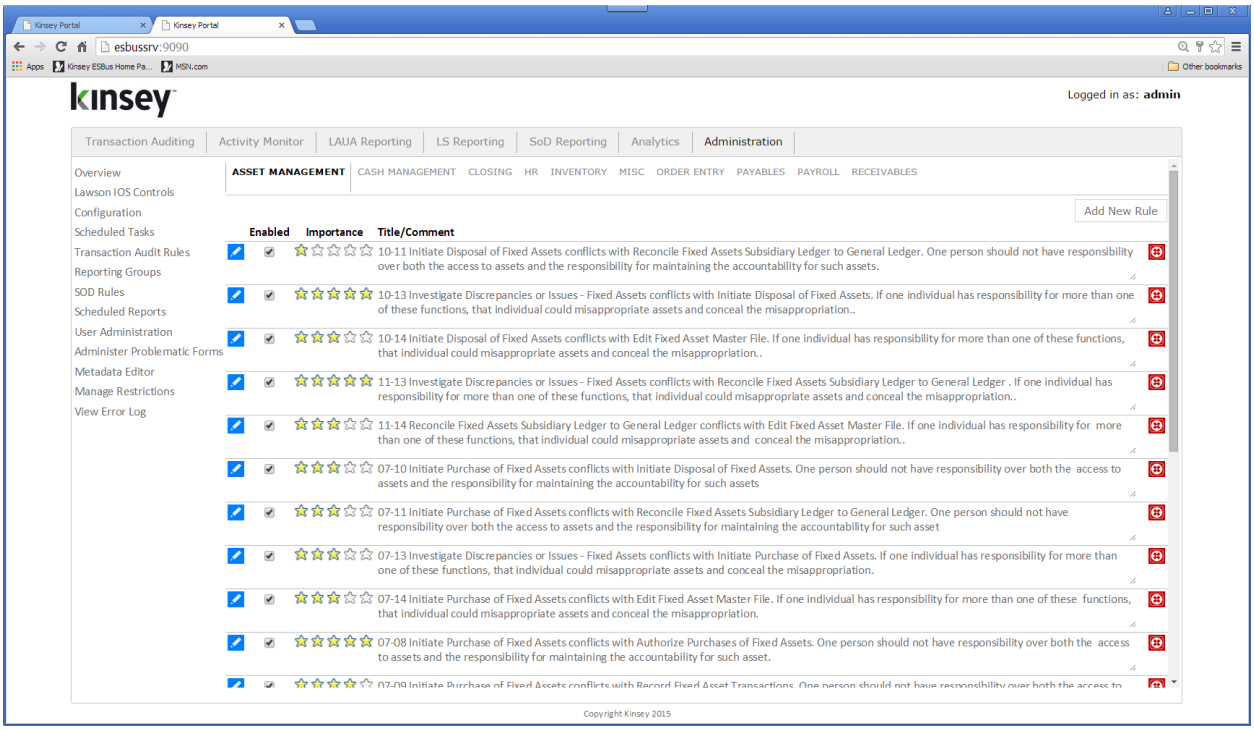
SOD Policy Maintenance

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 **SOD Policies** from the links on the left.

SOD Policies and Rules



The delivered policies are divided in to 8 categories. Additional categories can be added to hold any other policies that do not fit into one of the existing categories.

Enabling/Disabling a Policy

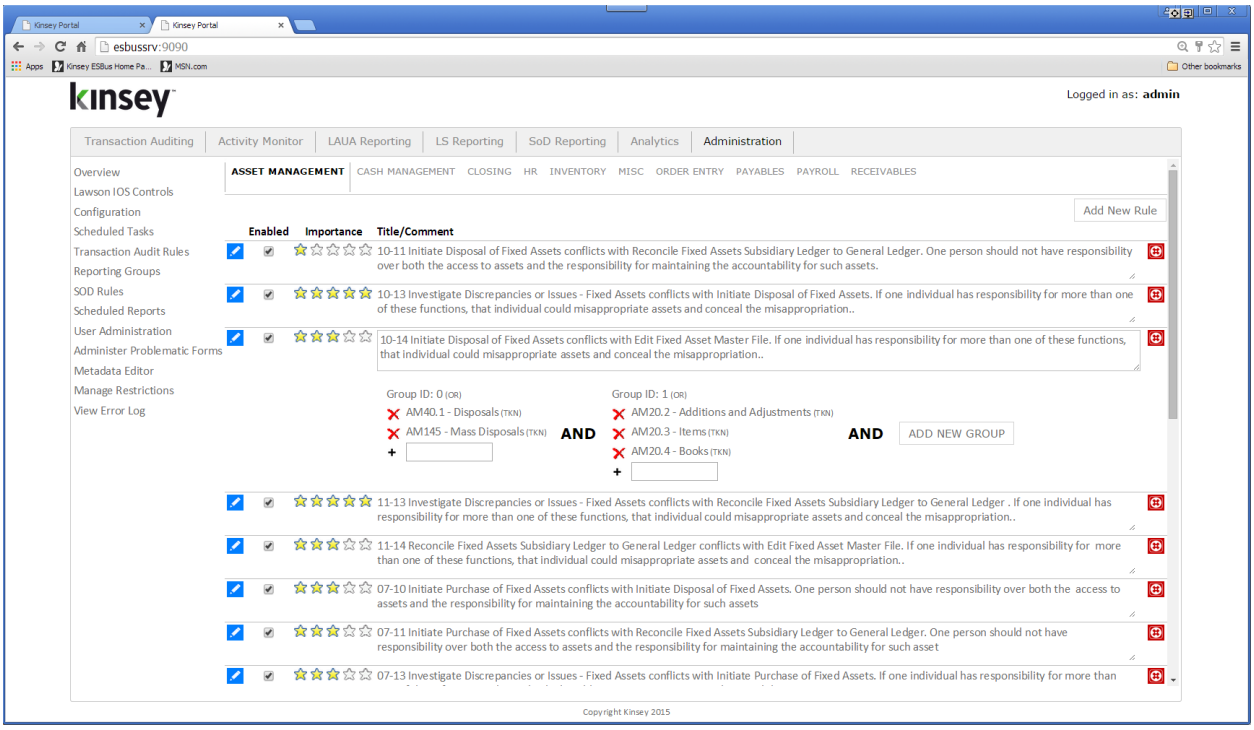
Each policy can be permanently disabled by un-checking the 'Enabled' check box. Any policy that is disabled will be removed from the SOD report. To enable a policy check the appropriate box next to the policy.

Rating a Policy's Level of Importance

The system will display the 8 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 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 3 and 2 objects respectfully. When evaluating this policy the application will validate your security setting against 6 rules.

The user is in violation of the policy if:

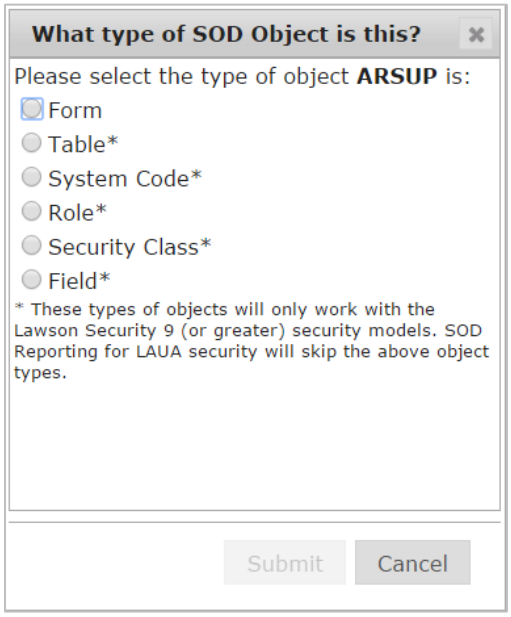
The user as access to AM12.1 and AM145 or
The user as access to AM12.1 and AM40.1 or
The user as access to AP20.1 and AM145 or
The user as access to AP20.1 and AM40.1 or
The user as access to PO20.1 and AM145 or
The user as access to PO20.1 and AM40.1 or

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

Note: Only 'Update' access is considered to be a violation of a policy. If just Inquiry function codes are granted for a token that has add, change or delete capabilities, then the token is considered to have NO ACCESS. For example form AM12.1 has available function codes A,C,D,I,N,P,+,-. If you restrict access to AM12.1 to just I,N,P,+,_ the SOD report will not consider this form to be in violation of the policy. Refer to the "Inquiry-only special exceptions" section of this manual for more information.

Adding a Object to an existing policy

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 a 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.*

Deleting an Object from an existing policy

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

Adding a Group to an existing policy

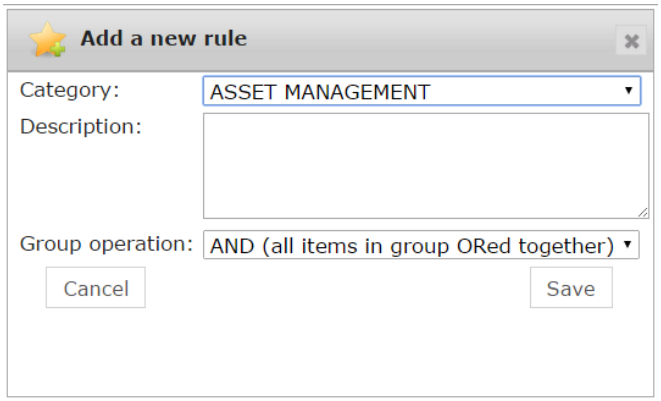
To add a new Group to a policy click on the ADD NEW GROUP button and fill in the appropriate object ID's.

Deleting a Group from an existing policy

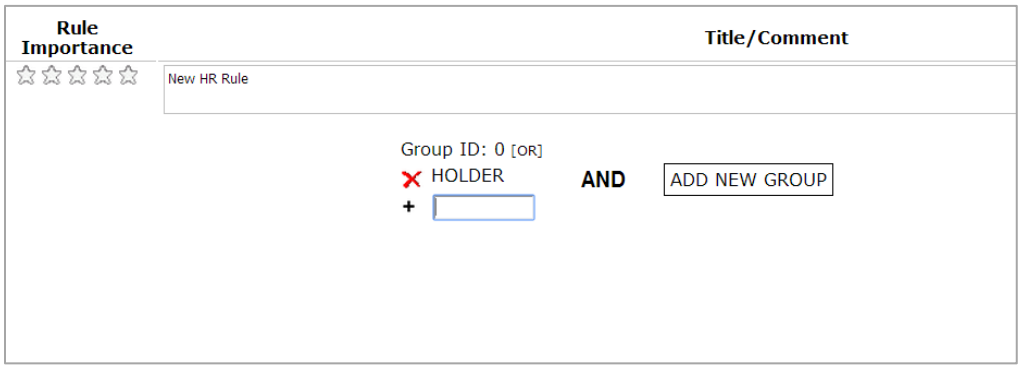
To delete a Group simply delete every object in the group and refresh your browser page.

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 right corner of the SOD screen.



You need to enter a policy description, category and group operator 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 entering the object ID's in Group 0 as described in the "Adding an Object" section. When you are finished with group 0 delete the object named "Holder'. You can then Add a New Group and assign the appropriate objects to Group ID 1.

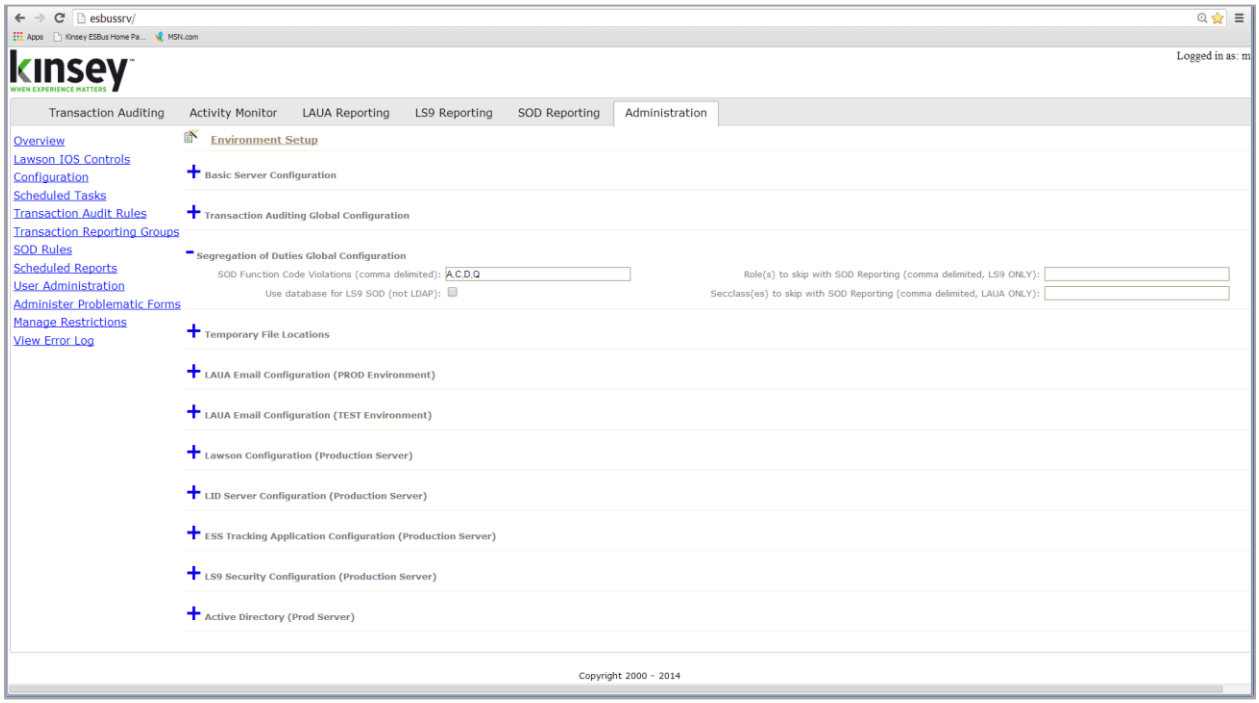
Note: When you are finished building your new policy remember to make sure it is enabled and rated.

Deleting a Policy

To remove a policy permanently you need to delete every object assigned to the policy and refresh your browser page.

SOD Configuration

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 or LAUA security class 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 LS9 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 LS9 SOD (not LDAP) – this option should be checked.

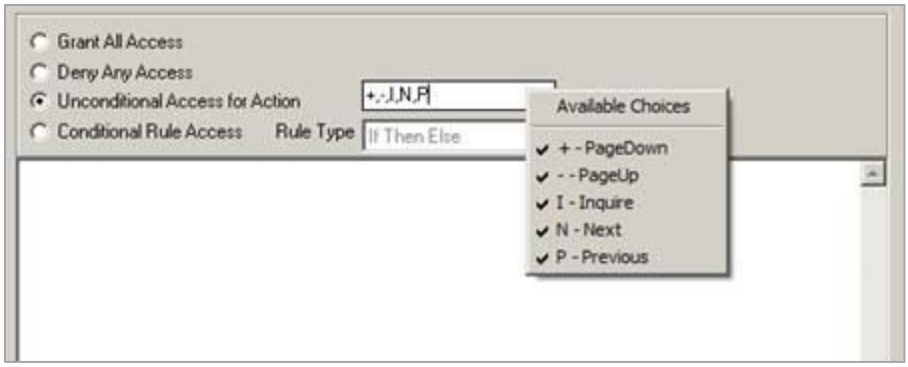
Exceptions for Inquiry-Only Forms

LAUA Security

If a token has been changed to restrict access to FC's A, C and D then that token is treated as though it has No Access and will not cause a violation. However, if a token's *only available function codes* are for inquiry access (i.e. PA51.2 only has +-I), and it's included in a rule, then we consider that token to have full access and it will cause a violation. The only way to prevent a token that does not have the FC's A,C,D in its profile from causing a violation is to delete the token from the SOD rule.

Lawson Security 9/10

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 it only has *inquiry* FC's. However if you put FC's in the "Unconditional Access for Action" (which actually means "Screen Actions Allowed") on 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 setting the Unconditional Access rules to all that are available has the same net effect on security.

Recap

LAUA

- If you restrict access to FC's A, C and D on a token then it's is considered Inquiry-only and will NOT cause a violation…
- However, if an Inquiry-only token is granted access then it WILL cause a violation regardless of the FC's provided.

LS

- 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…
- Or if an Inquiry-only token is setup with "Unconditional Access for Action" of only INP+- then it will NOT cause a violation…
- However, if an Inquiry-only token is setup as Grant All Access then it WILL cause a violation.

Note: For Kinsey's SoD application Inquiry-only is defined as a token that does not have ACD FC's available.

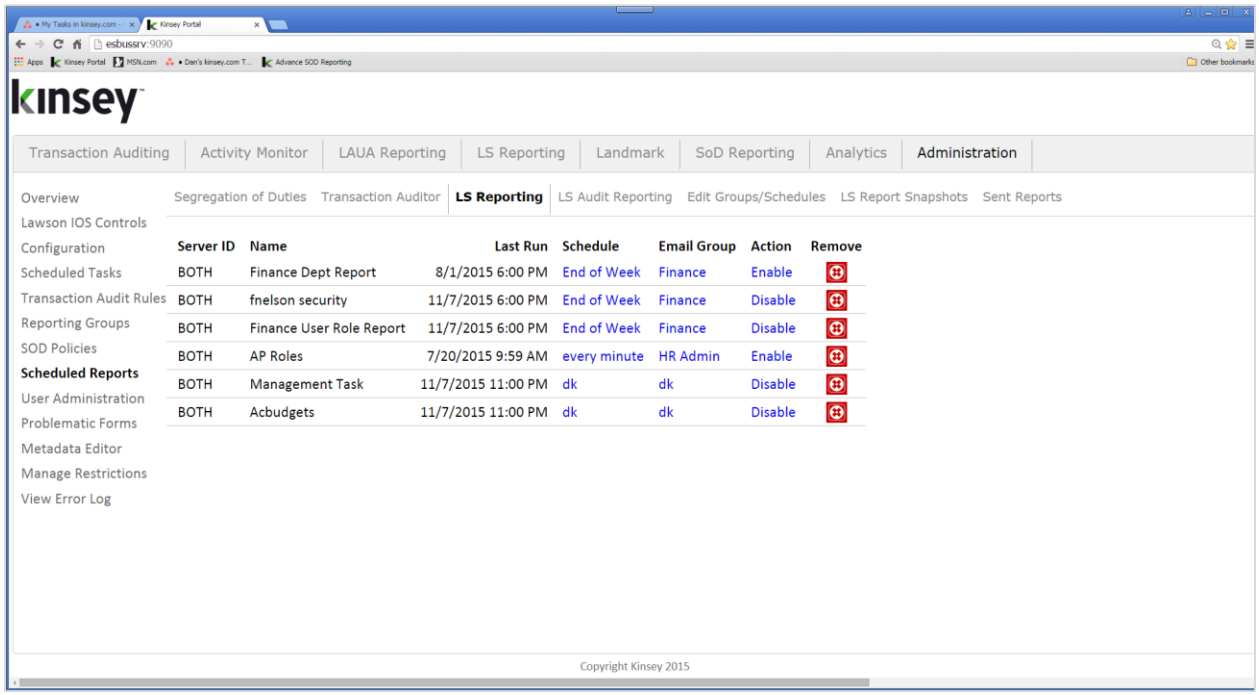
Note: The function codes A, C and D are default settings. The actual function codes used by the SoD application are defined in the SOD Function Code Violations field explained on page 12.

Scheduled Reports

The Scheduled Report option allows a administrator to Enable or Disable a schedule already assiged to the report for Transaction Auditing, Security Auditing, LS Reporting and SoD Reports. Additionally you can maintain the saved schedules and reporting groups through this option.

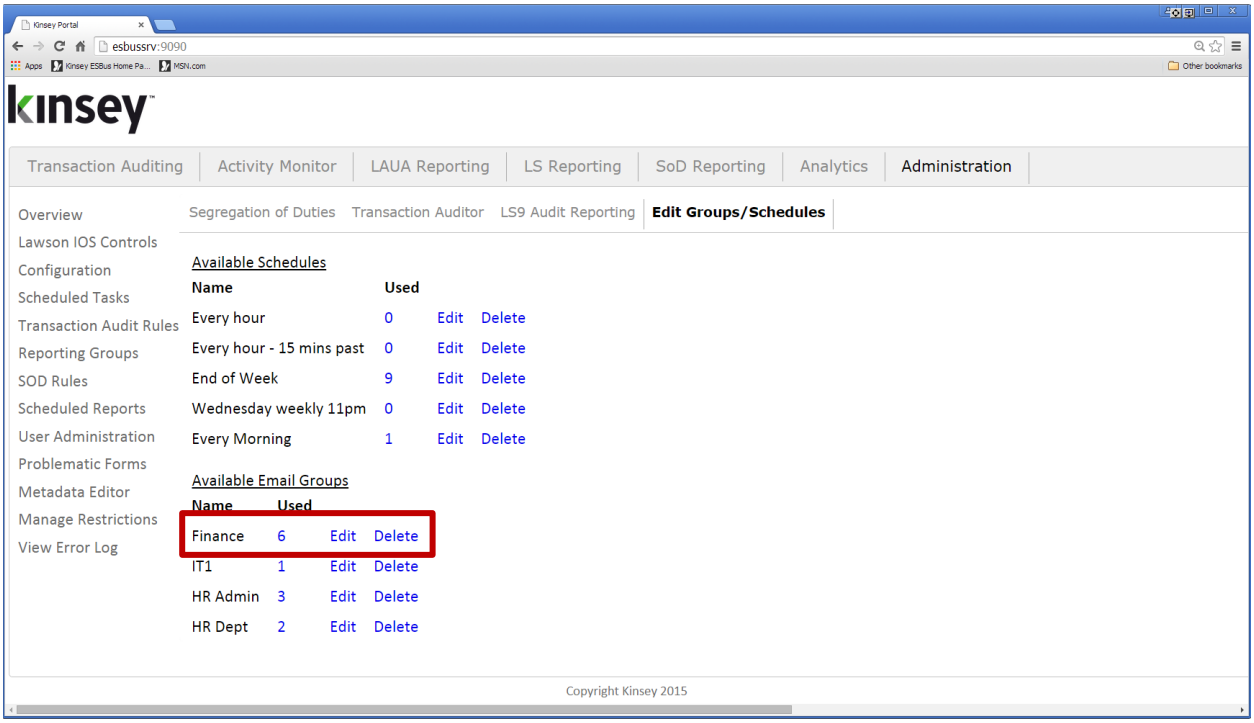
Enabling or Disabling a Scheduled Report

Using the Administrator tab on the home page select Schedule Reports. The 'Action' column on the right provides the option you can set the schedule to. For example in order to enable a schedule you must select the ENABLE link. The link is NOT reflective of the current status. The link indicates the action you want to take.

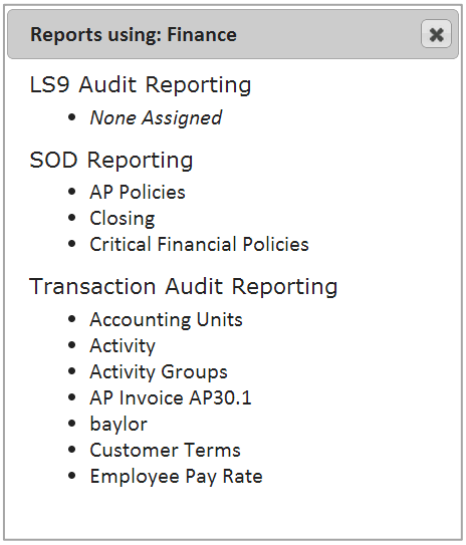


Editing Email Groups

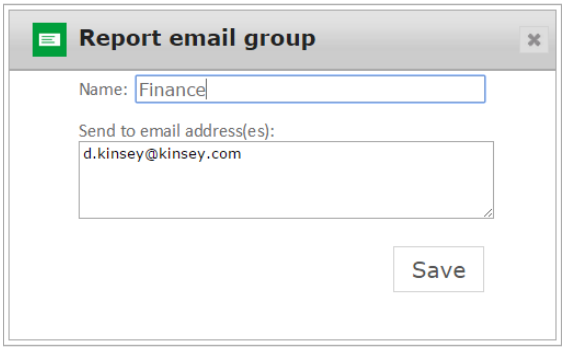
Select the Edit Groups/Schedule tab from the Administration > Scheduled reports link. Email Groups hold of list of emails address for report distribution. When a report is scheduled in either Transaction Auditing, Security Auditing or Segregation of Duties you can select a email group for automatic distribution.



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.

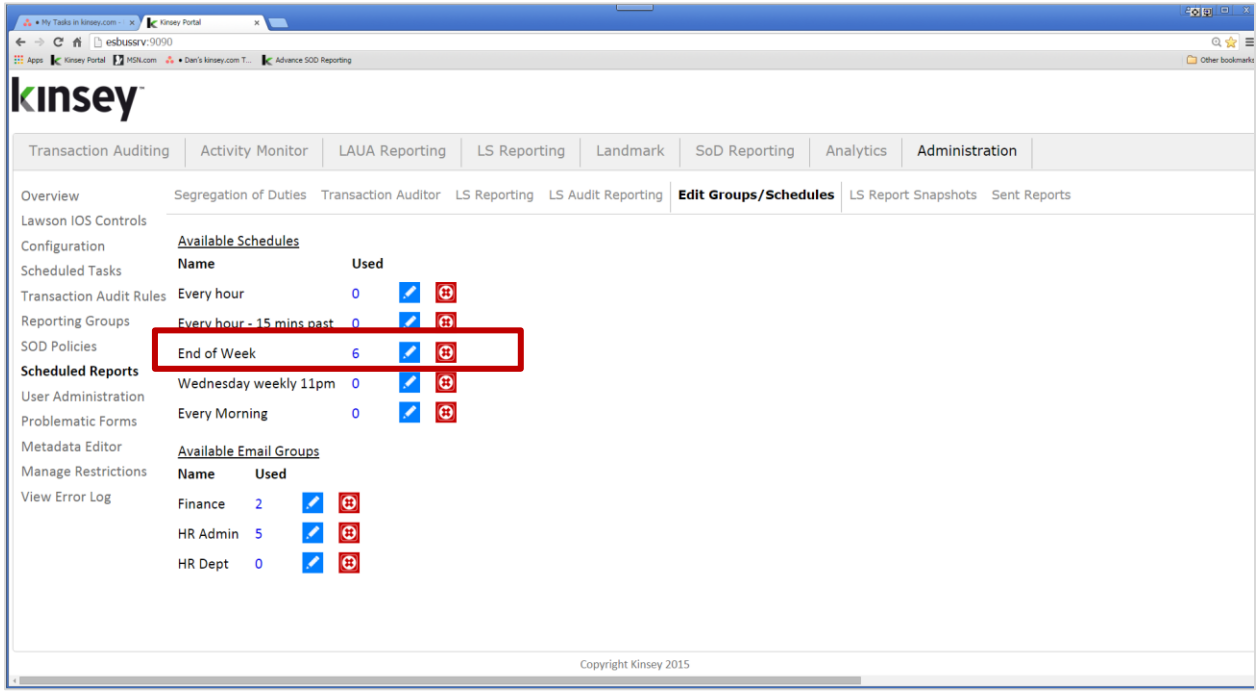


To change the email address asigned to the group select the Edit link.

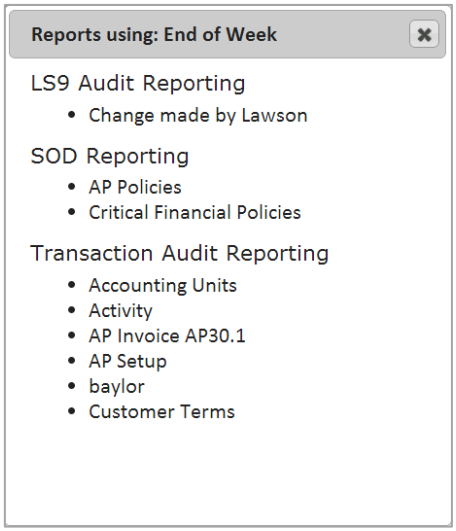


Editing Schedules

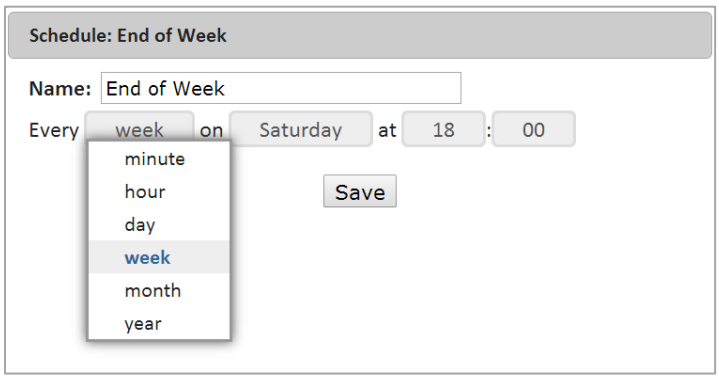
Select the Edit Groups/Schedule tab from the Administration >> Scheduled reports link. Schedules are used to determine when reports are generated and distributed for Transaction Auditing, Security Auditing or Segregation of Duties.



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.



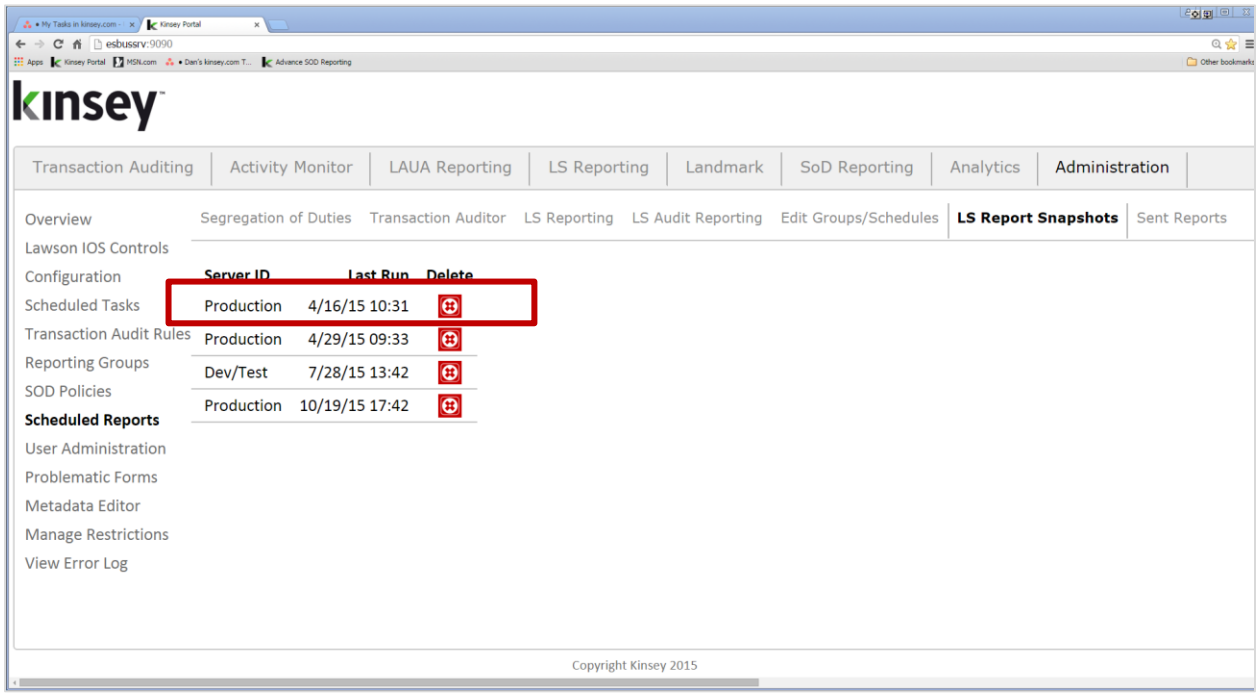
To edit and existing schedule select the Edit link and make the appropriate changes to the Period, Date and Time.



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

LS Report Snapshots

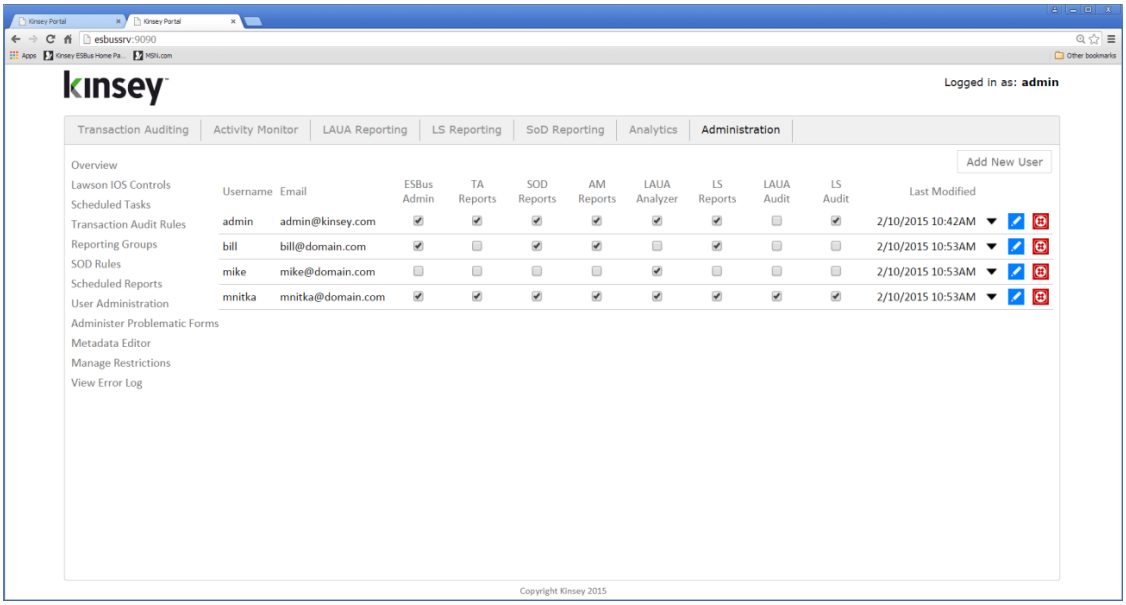
Select the LS Report Snapshots tab from the Administration >> Scheduled reports link. Snapshots are created through the scheduled task option by either setting up a schedule or manually running the task.



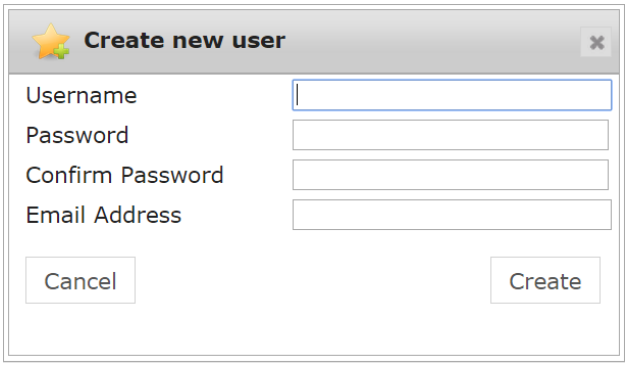
To delete a snapshot select the delete icon next to the desired row.

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.



To add application users enter the user name and password and select create. By default the user will not have access to any of the applications. Check the appropriate box to enable an application.

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

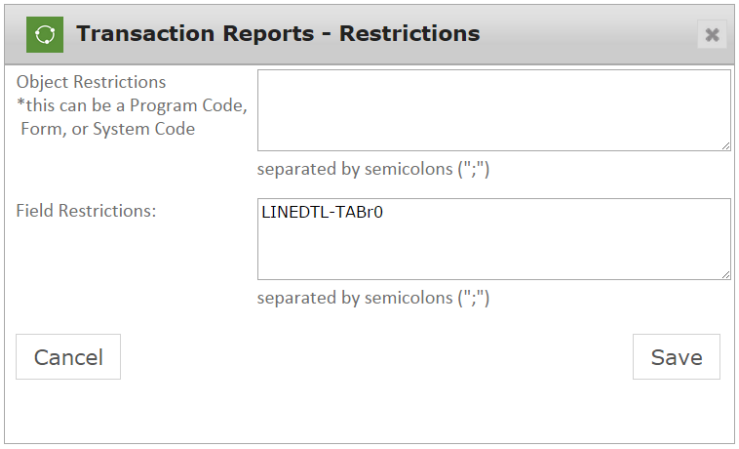
Detailed Application Security Settings

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

Report Restrictions

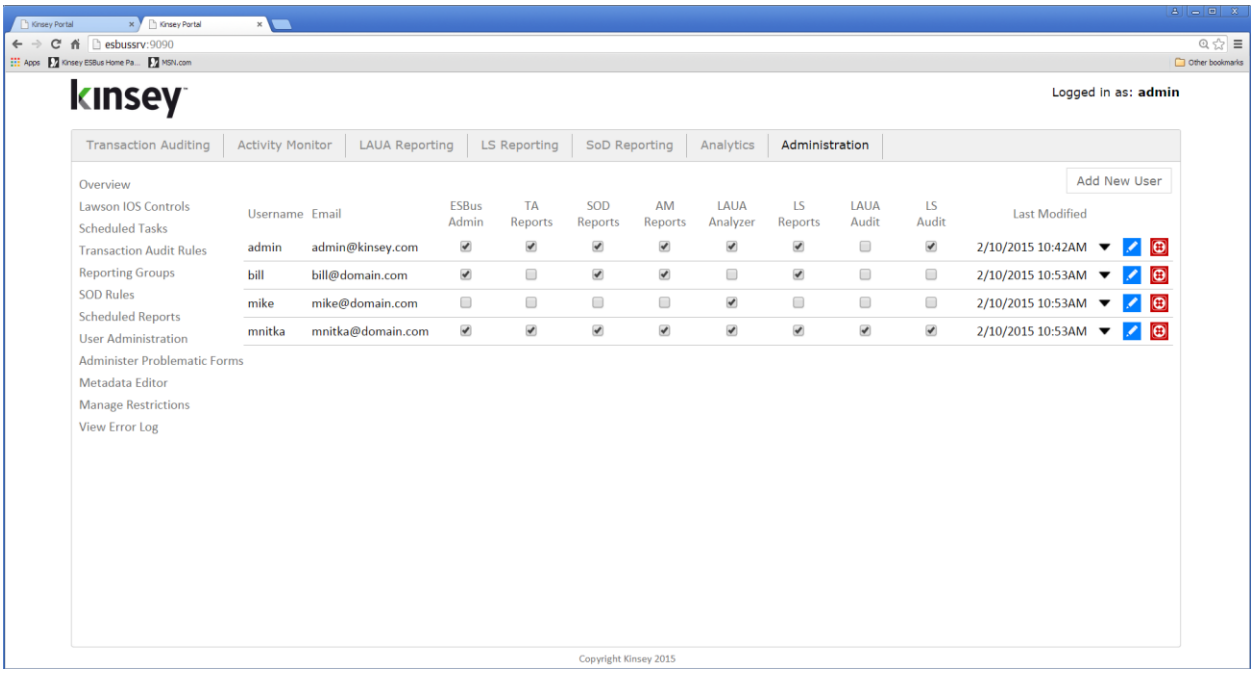
User Report Restrictions allow you to block forms or fields from being displayed in Transaction Auditing reporting, however the data you are restricting still exist in the audit database. The purpose of this feature is to hide information from users you might not want them to see. Since we allow you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

For those users setup with LAUA security this is the only way to hide data for a specific form. For any user setup through Security 9/10 the system will restrict a user from viewing any data related to a form they do not generally have access to. However, this is the only method available to secure data on a form from being viewed.



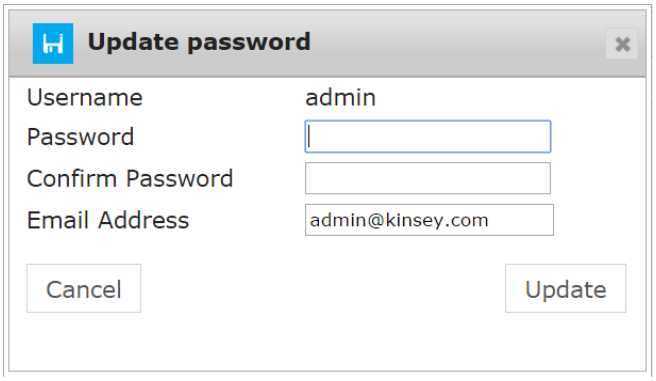
Changing or Deleting a User

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



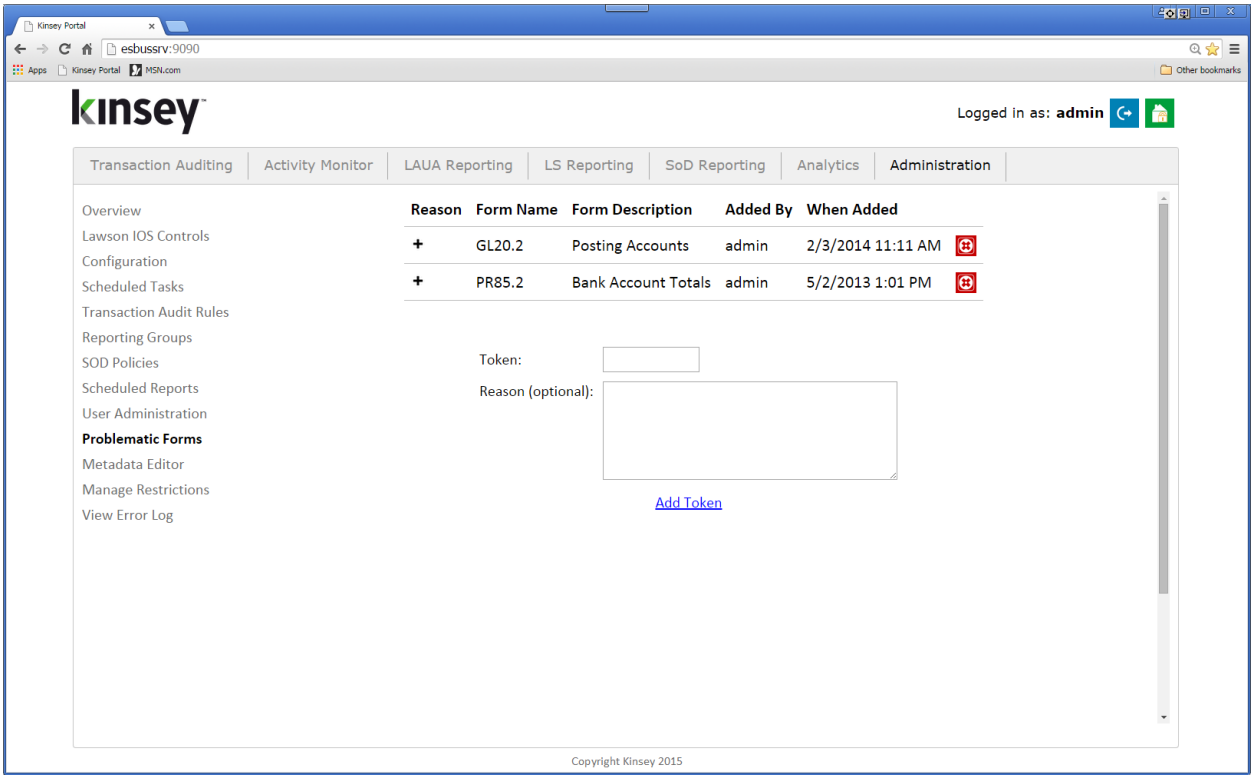
Note: the email address associate with the user is currently not currently utilized by any of the application.

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

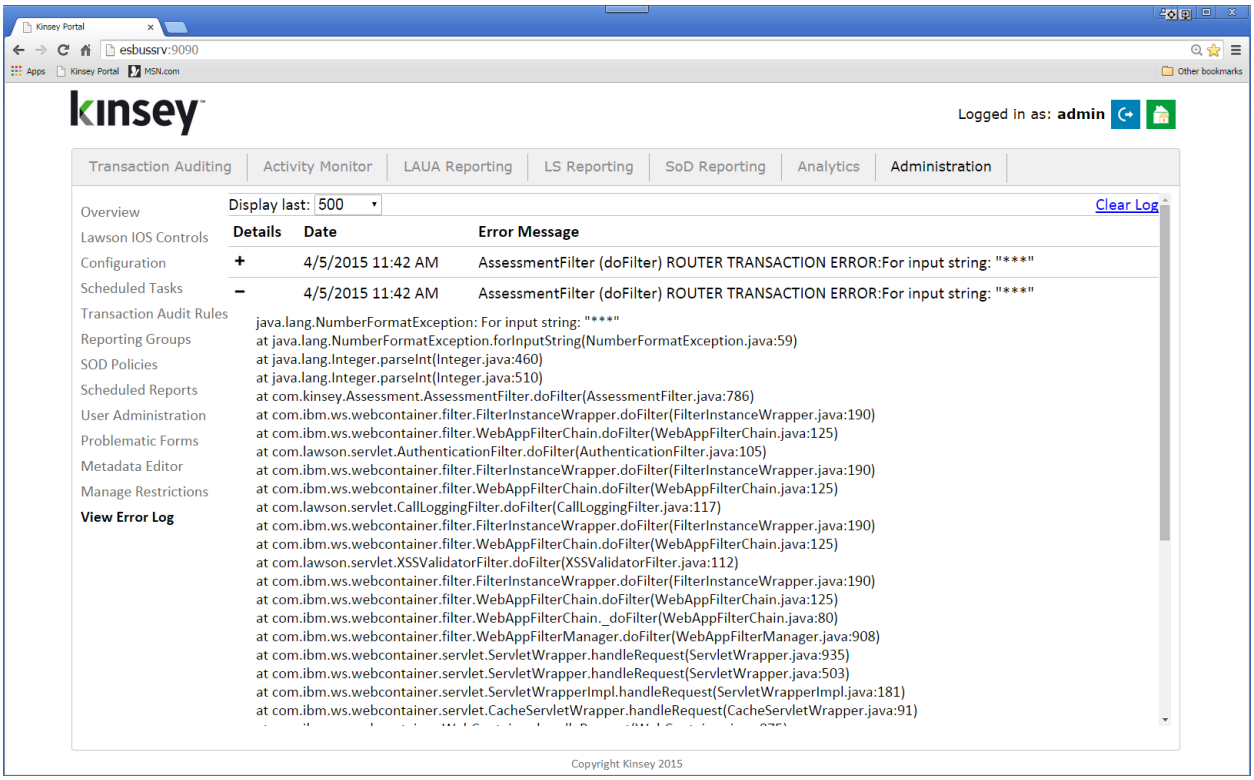


Administer Problematic Forms

The purpose of administering problematic forms is to prevent possible reporting errors on data collected via Transaction Auditing or Activity Monitor. On rare occasions we experience problems filtering out data for specific forms. This is turn causes the auditing application to return invalid results. We see this mainly with custom forms but there have also been some Lawson forms on older versions that cause problems. When these forms are identified they can be entered in to this screen and the TA and AM modules will skip the tokens until the problem can be resolved.



View Error Log



Commonly Ask Questions

Administrative

How do I deactivate the Listener Application or Transaction Auditing?

Refer to the back out procedures in the Listener 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 can first check to see if the MySQL and Tomcat processes are running on the Kinsey server and manually restart them, however 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 do I remove an LAUA Security Class from appearing on the LAUA SoD report?

You can manage the Security Classes through Administration > Configuration > Segregation of Duties Configuration; SecClasses to skip with SOD Reporting

How can I enable LAUA SoD Reporting?

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

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 security in the LS Reports?

The LS report dashboard collects the data from LDAP on a nightly schedule. Changes made during the day will not be included in the reports until the collection process is run. You can manually run the process through the Administration > Scheduled Tasks > com.esbus.appliance.collection_for_LS9Reporting.GetLDAPSecurity_TimerTask for either Production or Test

Why don't I see my changes to Lawson security in the LS Analyzer?

The LS report dashboard collects the data from LDAP on a nightly schedule. Changes made during the day will not be included in the reports until the collection process is run. You can manually run the process through the Administration > Scheduled Tasks > com.esbus.LS9Report.LS9Analyzer_LDAPDataCollection_TimerTask for either Production or Test

Why don't I see my changes to Lawson security in the LS Security Audit Report?

The LS9 security report collects the data from Lawson'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. You can manually run the process through the Administration > Scheduled Tasks > com.esbus.appliance.ls9_auditing.LS9Security_Audit_DB_TimerTask for either Production or Test.

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 Listener is running?

You can view activity counts for the past 5 minutes, 30 minutes, 4 hours or 24 hours through the Administration > Overview link for either the Production or Test server.

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); Listener Data Retention Time.

LAUA Reporting

Why don't I see my changes to LAUA security in the Reports?

The LAUA report collects the data from LAUA on a nightly schedule. Changes made during the day will not be included in the reports until the collection process is run. You can manually run the process through the Administration > Scheduled Tasks > com.esbus.appliance.serverUtil.GetLawsonListuserMap_TimerTask for either Production or Test

Problem Resolution

Kinsey recommends the installation of a virtual server (appliance) to host the Kinsey applications, Tomcat, Java and a MySQL database. The MySQL 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 appliance. This is only the case for customers running Transaction Auditing, Activity Monitor or Listener. All security migration projects will run the listener for a period of time, so if your company has engaged Kinsey for security work then the Listener is probably running.

The Lawson metadata is used strictly for Kinsey reports. This includes information like form 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. Instructions on updating the metadata tables can be found in the Administration Guide.

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 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. Instructions on updating the client tables can be found in the Administration Guide.

Transaction Auditing and Activity Monitor (Listener) data is collected real time. There is not a scheduled task for these processes.

Virtual Server System Settings

1. JVM Memory (relates to LAUA Reporting and 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. We base the setting on the number of LAUA classes defined. Generally 1.5GB will handle up to 100 LAUA Security Classes. However, this parameter can be a moving target depending on the OS and the amount of total memory allocated to the virtual appliance. If we over allocate JVM memory we run the risk of stealing resources from the server, however if we under allocate memory the LAUA reporting applications could hang the appliance. Proper system settings can only be obtained by running test setting in a test environment.
2. Appliance Memory (6 MB min)
    - This is a minimum requirement and can vary greatly depending on the OS and the size of the customers 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 appliance is fully operational prior to starting Lawson. More specifically, Tomcat and MySQL must be running on the appliance. Kinsey's WebSphere application will try to connect to the Kinsey appliance and retrieve configuration settings stored in MySQL. If a connection cannot be made, Lawson's Portal application will not respond correctly.

Note: The Kinsey appliance can be restarted anytime without stopping Lawson. When the Kinsey appliance 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 appliance is running, if not start the appliance and validate that you can access the Kinsey portal page.
2. Restart MySQL and Tomcat on the appliance in that sequence and validate that you can access the Kinsey portal page..
3. If Lawson still won't start then reboot the appliance and validate that you can access the Kinsey portal page.
4. If Lawson still won't start then deactivate Listener (refer to page 8 of Kinsey Summarized Installation Guide)

If Listener needs to be deactivated please schedule time with Kinsey to evaluate the condition of the appliance 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 appliance. If the Kinsey server is unable to received messages for any reason the JMS queues will hold the transactions until the Kinsey appliance is back online. This is similar to an email message being stuck in an outbox. If the Kinsey appliance 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 appliance is back online all of the messages (transactions) will be sent to the appliance.

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.

Notes: