

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
Lawson IOS Controls
Configuration7
Basic Server Configuration7
Transaction Auditing Global Configuration7
Segregation of Duties Global Configuration9
Lawson Configuration Production Server10
LID Server Configuration (Production Server)11
ESS Tracking Application Configuration (Production Server)11
LS9 Security Configuration (Production Server)11
Lawson Configuration Test Server12
LS Security Configuration (TEST Server)12
Scheduled Tasks
Defining a Schedule16
Transaction Audit Rules
Assigning or Removing a User to a Group
SOD Policy Maintenance
Enabling/Disabling a Policy23
Rating a Policy's Level of Importance23
Viewing or Editing a Policy23
Adding a Object to an existing policy25
Deleting an Object from an existing policy25
Adding a Group to an existing policy25
Deleting a Group from an existing policy25
Creating a New Policy
Deleting a Policy
SOD Configuration
Scheduled Reports
Enabling or Disabling a Scheduled Report
Editing Email Groups31
Editing Schedules32
LS Report Snapshots
User Administration
Administer Problematic Forms
VIEW LITUI LUY

29 Administrative	9 19
Segregation of Duties	9
LS Reporting4	0
Activity Monitor (Listener)4	1
LAUA Reporting4	1
Problem Resolution	.2 2
Potential Lawson Issues	3
Virtual Server Monitoring44	4
LS Reporting Data Collection Problems4	-5

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

Authentication	Authentication Required						
The server http://e password. The serv	sbussrv:80 requires a username and /er says: ESBus Admin.						
User Name: Password:							
	Log In Cancel						

Enter your administrative User name and Password

Overview

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

Portal × 🕅 Kinsey Port	el .	×									
🕈 🏠 esbussrv:9090											
Kinsey ESBus Home Pa 🚺 MSN.com											<u> </u>
kinsey										Logged in as: a	admin
Transaction Auditing Ac	tivity Monito	or LAUA F	Reporting	LS Reporting	SoD Rep	orting Ar	alytics Ac	ministration			
Overview	Lawson Serv	er: Select Se	rver 🔻								
Configuration	Listener Filte	er Processing (in seconds) - up	dated every	30 seconds				Appliance Stats		
Scheduled Tasks Transaction Audit Rules			Last 5 mins La	st 30 mins La	ist 4 hrs Last 24	4 hrs			Operating System:	Linux ver 3.10.0-123.13.2.el7.x86_64 - amd64	
Reporting Groups	Lawson IOS	Filter (avg)							Config Database:	MySQL ver 5.6	
SOD Rules	Lawson IOS	Filter (min)							Storage Database:	MySQL ver 5.6	
Scheduled Reports	Lawson IOS	Filter (max)							Database Table Record F	Setimates - undated even 60 seconds	
User Administration	Lawson IOS	Transactions							Database Table Record Estimates - updated every ou seconds		
Administer Problematic Forms	Transaction	Audit Filter Pr	ocessing (in sec	onds) - undat	ted every 30 se	conds			Auditing Database		
Manage Postrictions			occosing (in occ	onast apaa	ica crei y so se	contas			Header Records:		
View Error Log			Last 5 mins La	st 30 mins La	ist 4 hrs Last 24	4 hrs			Detail Records:		
	Lawson IOS	Filter (avg)							Listener Database		
	Lawson IOS	Filter (min)							User Summary:		
	Lawson IOS	Filter (max)							User Detail:		
	Lawson IOS	Transactions							LAUA Prod Server Datab	1352	
	IME Quotion	Current Roce	vede						Allowed Forms:		
	Juis Queues	- current kett	705						LAUA Test Server Databa	ase	
	Transaction								Allowed Forms:		
	Transaction	Error									
	Re-sending I	Error									
	Generic Erro	or									
	Database Co	nnections - up	dated every 30	seconds							
	GEN	AUDIT	INTERNAL	LAUA	LAUA (T)	LS9	LS9 (T)	SESSION	USAGE		
	Total:2	Total: 10	Total:4	Total:3	Total:3	Total: 2	Total:3	Total:2	Total:2		
	Idle: 0	Idle: 8	Idle: 2	Idle: 3	Idle: 3	Idle: 2	Idle: 3	Idle: 2	Idle: 0		

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.

Transaction Auditing Ac	ctivity Moni	tor LAUA Reporting LS Report	ting SoD Reporting Analytics Administration	
Overview Lawson IOS Controls	Lawson S	erver: Select Server •		
Configuration Scheduled Tasks	IOS Relat	ed Functions		
Transaction Audit Rules	Success	Command	Description	
Reporting Groups		Reload Environment Variables	Reload environment variables in the IOS aplication from Kinsey Application server. This includes updated settings and appliance server changes.	
Scheduled Reports		Reload Lawson Metadata	Reload token and function code maps and cache.	
User Administration		Refresh Session Manager Restrictions	This will reload the session manager restrictions. Changes, additions, etc.	
Administer Problematic Forms		Add Servlet Filters	Turn on Listener and/or Auditor by adding servlet filters to the Lawson IOS application.	
Metadata Editor		Remove Servlet Filters	Turn off Listener and/or Auditor by removing servlet filters from the Lawson IOS application.	
View Error Log				
-	Auto-Ren	noval of servlet filters from the La	wson IOS application	
-	Auto-Ren Enable ser	vlet filters to be removed automatically:	wson IOS application No • Current average servlet filter time:	
-	Auto-Ren Enable ser Set limit of	Noval of serviet filters from the Land vlet filters to be removed automatically: f seconds on 10 JMS messages:	No Current average servlet filter time: 5 seconds •	
	Enable ser	Noval of serviet filters from the Larviet filters to be removed automatically: f seconds on 10 JMS messages:	seconds vertication Current average servlet filter time: 5 seconds	
-	Auto-Ren Enable ser Set limit of	noval of servlet filters from the La vlet filters to be removed automatically: f seconds on 10 JMS messages:	woon IOS application No Current average servlet filter time: 5 seconds •	
-	Auto-Ren Enable ser Set limit of	noval of serviet filters from the La Viet filters to be removed automatically: f seconds on 10 JMS messages:	wson IOS application No Current average servlet filter time: 5 seconds •	
-	Auto-Ren Enable ser Set limit of	moval of service titlers from the La Viet filters to be removed automatically: { seconds on 10 JMS messages:	wson IOS application No Current average servlet filter time: /5 seconds •	
-	Auto-Ren Enable ser Set limit of	noval of service titlers from the La Viet filters to be removed automatically: f seconds on 10 JMS messages:	wson IOS application No Current average servlet filter time: 5 seconds •	
	Auto-Ren Enable ser Set limit of	noval of service titlers from the Lai viet filters to be removed automatically: (seconds on 10 JMS messages:	wson IOS application No Current average servlet filter time: 5 seconds •	
	Auto-Ren Enable ser Set limit of	noval of service titlers from the La vlet filters to be removed automatically: (seconds on 10 JMS messages:	wson IOS application No Current average servlet filter time: 5 seconds •	
	Auto-Ren Enable ser Set limit of	noval of service titles from the La	woon IOS application No Current average servlet filter time: 5 seconds 	

Configuration

Basic Server Configuration

Customer Name Kinsey	y and Kinsey	Reload Required on LSF Agent	
ESBus Home /var/tom	mcat/webapps/esbus	ESBus Administrator	mnitka
ESBus User lawson	n	ESBus Password	•••••
Update KK at Message Level 1 - ER	ROR		
ESBus Start Time 8		Default Error Page	http://localhost/esbus/error.htm
Permissable IP Patterns *****		Catastrophe Handler	
ESBus Server Name http://loo	ocalhost	Destroy Class	esbus.globalPlugs.SampleShutDownClass
No Map Caching 🗹		System Debug	
		Debugging Level:	9 •
Start Location /var/tom	mcat/webapps/esbus	ESBus Admin Portal URL	http://192.168.100.136
Is this server hosted: 🔲			

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.

Transaction Auditing Global Configuration		
Auditing Enabled: 🗹	Store audited DME Data: 🔲	
Listener Enabled: 🗹	Store audited IDA Data:	
Auditing/Listener Stats Retention Time: Delete after 14	days Skip these URI's in Auditor (seperated by semicolons): sso/SSOServlet 	
Use LDAP attribute for Reporting Groups: 🔲	Use Transaction Security 🗹	

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.

Segregation of Duties Global Configuration		
SOD Function Code Violations (comma delimited): (A,C,D,Q	Role(s) to skip with SOD Reporting (comma delimited, LS9 ONLY):	
Use database for LS9 SOD (not LDAP):	Secclass(es) to skip with SOD Reporting (comma delimited, LAUA ONLY):	

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 LD	DAP) – Check this option if you want the SOD reports to use the Kinsey LS SQI 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 us	se 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.

Temporary File Locations	
LS9 Analyzer	/var/tomcat_9090/webapps/LS9_Report/tmp/
LAUA Audit Reports	/var/tomcat_9090/webapps/LAUA_Report_Changes/tmp/
SOD Reports	/var/tomcat_9090/webapps/SOD_Report/tmp/
LAUA Reports (Excel Based)	/var/tomcat_9090/webapps/LAUA_Report/tmp/
LS9 Reporting	/var/tomcat_9090/webapps/KK_LS9ReportingPortal/tmp/
ROOT	/var/tomcat_9090/webapps/ROOT/tmp/

Lawson Configuration Production Server

This information will be configured on installation.

Lawson Configuration (Production	n Server)		
ESBus Server ID	LSF_PROD		
Lawson Server			
Lawson Product Line	LIVE	Lawson New Port	
Web Server	http://ls3server.corpnet.lawson.com	Web User	lawson
Web Password	•••••	TranMap Home	/var/tomcat/webapps/esbus/ser_maps/
Serialized Maps	/var/tomcat/webapps/esbus/ser_maps/	Lawson Foundation 9	CGI 🗹 ERP
Use for Listener Sec Class		Use LAUA SQL Tables for Sec Class	
Enabled for SOD Reporting		Security Model:	LS9 🗹 LAUA 🗹
Enable ASYNC HTTP Calls (instead of JMS):		Lawson Server OS:	Windows •
KK Lawson Portal Application URL	http://ls3server.corpnet.lawson.com:9080/KKL	awsonFilterPortal	
Listener Data Retention Time:	Delete after 180 days •	If multiple data areas (make map): [prodline]=[data area] mapping, seperated by semicolon	MJN=LIVE;
Try to do a DNS lookup:			
Restrict Users in LS9 Reporting by CHECKLS:			

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.

LID Server Configuration (Production Server	r)		
LID Token XML File Location:	/var/tomcat/webapps/esbus/LawTranMaps		
'Tombstone' Timeout (ms):	43200	Local port to receive IPFilter file	42000
Lawson Server IP:	10.20.50.104	Lawson Server Port	23
Lawson (default) Prod Line:	LIVE	Connection clean up frequency (secs)	30
Valid Product Lines (separated by Semicolons ";"):	LIVE;TEST	What to look for as valid login	: Last login:
AIX IPReport File Path (optional):	/var/tomcat/webapps/esbus/Temp/trace.report		

ESS Tracking Application Configuration (Production Server)

This form is currently not in use.

ESS Tracking Applicatio	n Configuration (Production Server)
Active Employee DME	"SELECT" Option:
	ESS Prod Line: LIVE

LS9 Security Configuration (Production Server)

This information will be configured on installation.

LDAP Server:	ls3server.co	orpnet.lawson.com		LDAP User:	CN=root,CN=lwsn,DC=ls3server
LDAP Port:	389			LDAP Password:	Lawson1975
LDAP Base Search:	CN=lwsn,D	C=Is3server		LDAP Profile:	APS
User LDAP Base Search:					
LDAP Paging Size:	1000			RMID Translation Productline:	
LDAP "back- office" Service:				LDAP "Company:Employee" Service:	LIVE_EMPLOYEE
Collect Employee termination data:				LS Audit DB (TABLE.SCHEMA):	LOGAN.LSAUDIT
Employee fields to collect:	COMPANY	;EMPLOYEE;DATE_HIRED;TERM	_DA		
LS Security	Hidden	Friendly Name Da	abase Field		
Fields:		Attribute A	TRIBUTE		
		Attribute Value A	TRIBUTE_VALUE		
		Audit Au	JDITED		
		Available FC A	AILABLEFC		
		Check LS Cl	IECK_LS		
		Company Co	OMPANY		

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.

🗋 Kinsey Portal 🗙 🗋 Kinsey Portal	×		. O X
← → C ㎡ ㎡ 🗅 esbussrv:9090		(Q ಭ ≡
Apps 🚺 Kinsey ESBus Home Pa 🚺 MSN.com		🗀 oth	ner bookmarks
kinsey		Logged in as: admin	
Transaction Auditing Ac	tivity Monitor LAUA Reporting LS Reporting SoD Reporting Analytics Administration		
Overview Lawson IOS Controls	Create New Task	Í	
Scheduled Tasks	Enabled Task Class	Desc Edit Del Run Last Ran (mins)	
Transaction Audit Rules	com.esbus.appliance.collection_for_LS9Reporting.GetLDAPSecurity_TimerTask	2/9/15 17:00 3.845	
Reporting Groups	com.esbus.appliance.collection_for_LS9Reporting.GetLDAPSecurity_TimerTask_TEST	📄 🗾 🔁 💿 2/5/15 11:51 4.793	
Scheduled Reports	com.esbus.appliance.GetMisc_GEN_Tables_TimerTask	10/21/14 12:21 0.222	
User Administration	com.esbus.appliance.GetMisc_GEN_Tables_TimerTask_TEST	I/1/00 00:00 0.000	
Administer Problematic Forms – Metadata Editor	com.esbus.appliance.Get_FullName_From_LDAP_RESOURCES_TimerTask	Z 2/4/15 14:10 0.002	
Manage Restrictions	com.esbus.appliance.GrabToken_Definitions_TimerTask	Z (10/14 15:14 51.032)	
View Error Log	com.esbus.appliance.GrabToken_Definitions_TimerTask_TEST	1/1/00 00:00 0.000	
	com.esbus.appliance.LAUA_CommandLine_To_MySQL_TimerTask	11/4/14 14:24 0.205	
	com.esbus.appliance.LAUA_CommandLine_To_MySQL_TimerTask_TEST	11/4/14 16:00 0.488	
	com.esbus.appliance.ls9_auditing.LS95ecurity_Audit_DB_TimerTask	1/21/15 15:07 0.013	
	com.esbus.appliance.ls9_auditing.LS95ecurity_Audit_DB_TimerTask_TEST	1/21/15 15:18 0.001	
	com.esbus.appliance.ls9_auditing.LS9Security_Audit_LDAP_TimerTask	1/21/15 15:11 0.009	
	com.esbus.appliance.ls9_auditing.LS9Security_Audit_LDAP_TimerTask_TEST		
	com.esbus.appliance.monitoring.Cleanup_AuditorTables_TimerTask	11/4/14 00:00 2.822	
	com.esbus.appliance.monitoring.Cleanup_ListenerTables_TimerTask	 I ∠ 😟 🖸 11/4/14 00:00 1.038	
	com.esbus.appliance.monitoring.Cleanup_SessionTables_TimerTask		
	Copyright Kinsey 2015		

Applications: LS Reporting

Kinsey & Kinsey, Inc. Confidential 2008-2015 (v.0625)

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_T EST 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 Collects LS security data for TEST environment Purpose: 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 com.esbus.appliance.LAUA_CommandLine_To_MySQL_TimerTask Task: 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: Purpose:	LAUA Reporting, Activity Monitor, Transaction Auditor 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: Purpose:	LAUA Reporting, Activity Monitor, Transaction Auditor 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

Months(s):	Day(s):	Hour(s):	Minute(s):	Weekday(s):
Every Month	Any Day	Every Hour	Every Minute	Any Week Day
January	Every Day	Every Other Hour	Every Other Minute	Every Week Day
February	1	Every Four Hours	Every Five Minutes	Sunday
March	2	Every Six Hours	Every Ten Minutes	Monday
April	3	0 = 12 AM/Midnight	Every Fifteen Minutes	Tuesday
May	4	1 = 1 AM	Every Thirty Minutes	Wednesday
June	5	2 = 2 AM	0	Thursday
July	6	3 = 3 AM	1	Friday
August	7	A - A AM	2	Saturday
usk Description: pllect LS9 data (P	ROD)	appnance.conection_for_cs	oneporting.detLDAPSecurity_1	Enabled: e
and in a time of 1 CO R	eporting			

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.

Ch Kinsey Prytal	~														Ŀ	8) L_	. 🗆 🗙
	cenu:0	000															0 ch =
Apps I Kinsey ESBus Home P	Pa D	MSN.com														C ot	her bookmarks
																_	
kinsey														Logge	d in as	: adr	nin (+
Transaction Auditing	Ac	ctivity Monitor	LAUA Reporting	LS Reporting	SoD Reporting	Analytics	Administration										
Overview	Creat	te New Audit Rul	e Audit Rule Report														A
Lawson IOS Controls														1	Retent	on	- 1
Au Configuration	udit IC	D Description						Prod Line	User	Form/Token	Func Code	IP Address	Time	Server	INP A	CD	
Scheduled Tasks	110	AC Setup						-		Ŷ	Y	-	-	Both	-	-	
Transaction Audit Rules	42	ALL LIVE PRODLI	INE					Ť	-	-	-	-	Ŷ	Test	52 3	2 .	
Paparting Groups	67	AP Adjustments						-	-	ř	-	-	-	Both	4 :	2	
COD Bules	71	AP BII OF EXCITAT	ige					-		T	-	-	-	Both	4 3	2 . 2	
SOD Rules	66	AP Payments	pense							×				Both	4	52	
Scheduled Reports	65	AP Processing						-	-	Y	-	-	-	Both	4	52	
User Administration	69	AP Setup						-	-	Y	Y	-	-	Both	1 !	52	
Problematic Forms	70	AP System Code	!S					-	-	Y	Y	-	-	Both	1 !	52	
Metadata Editor —	75	AR Applications						-	-	Y	-	-	-	Both	4 5	52 🛃	
Manage Restrictions	77	AR Bill of Exchar	nge					-	-	Y	-	-	-	Both	4	52 🛃	
View Error Log	73	AR Cash						-	-	Y	-	-	-	Both	4 3	52 📝	2 🕀
	76	AR Electronic Fu	inds					-	-	Y	-	-	-	Both	4 3	52 📝	2 🕀
	72	AR Setup						-	-	Y	Y	-		Both	1 3	52 🛃	2 🕀
	74	AR Transactions						-	-	Y	-	-		Both	4 3	52 🛃	2 🕀
	111	BR Billing and Re	evenue Setup					-	-	Y	-	-		Both	4 !	52 🛃	2 🕀
	88	CB Cash Ledger	Setup					-	-	Y	-	-	-	Both	1 !	52 🛃	2 🕀
	89	CB Processing						-	-	Y	-	-	-	Both	4 5	52 🛃	2 🕀
	90	CB Processing - I	Interface					-	-	Y	-	-	-	Both	4 5	52 🛃	2 🕀
	91	CB Processing - I	Reconciliation					-	-	Y	-	-	-	Both	4 5	52 🛃	2 🕀
	84	GL Processing - J	Journal Entry					-		Y	-	-		Both	4	52 🛃	2 🕀
	86	GL Processing - (Other					-		Y	-	-		Both	4	52 🛃	2 🕀
	85	GL Processing - I	Period End					-	-	Y	-	-		Both	4	52 🧏	2 🕀
	79	GL Setup - Accou	unting Units					-		Y	Y	-	-	Both	4 5	52 🛃	2 🕀
	78	GL Setup - Comp	pany					-		Y	Y	-		Both	1 3	52 🛃	2 🕀 🗸
						Copyright I	Kinsey 2015										

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.

← → C file esbussrv:9090 C If None If None If None KINSEY [*] Transaction Auditing Activity Monitor LAUA Reporting LS Reporting SoD Reporting Analytics Administration	©, ☆ 〓
III Age Direct FERGE France Par Direct France Par Direct Par	C Other bookmarks
KINSEY* Transaction Auditing Activity Monitor LAUA Reporting LS Reporting SoD Reporting Analytics Administration	
Transaction Auditing Activity Monitor LAUA Reporting LS Reporting SoD Reporting Analytics Administration	
Overview Create New Lawson Auditing Rule Lawson IOS Controls Please separate multiple entries with "SEMI-COLON" [;] Configuration	
Scheduled Tasks Audit Rule ID: 71	
Transaction Audit Rules Lawson Servers: Both	
Reporting Groups Rule Description: AP Employee Expense	
SOD Rules Productline(s):	
Scheduled Reports User Name(s):	
User Administration Token(s): EESU.*;EE30.*;APPR.*;EE175	
Metadata Editor Function Code(s):	
Manage Restrictions IP Address:	
View Error Log Audit Start Time (hr/min): 0 • 00 • AM •	
Audit End Time (hr/min): 0 • 00 • AM • * Setting Start and End time to "0:00 AM" disables time constraint	
Copyright Kinsey 2015	

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.
	<i>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.)</i>
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

🗅 Kinsey Portal 🛛 🗙								
← → C ♠ esbussrv ∴ Apps	r:9090 							Q 🚏 🚖 ☰ ☐ Other bookmarks
kinsey								
Transaction Auditing	Activity Monit	Dr LAUA Reporting	LS Reporting	SoD Reporting	Analytics	Administration		
Overview	Transaction Audit	ng LS9 Auditing						
Lawson IUS Controls Configuration Scheduled Tasks Transaction Audit Rules Reporting Groups SOD Policies Scheduled Reports User Administration Problematic Forms Metadata Editor Manage Restrictions View Error Log	Edit groups Group Administrators a m Finance GL Accounting Auman Resource Payroll A GL	min (2) min (2) nitka (2) min (2) min (2) min (2)		Add us	ser to gra Username: S Administ Finance GL Accou Human R Payroll	elect User rators nting esource	×	
				Ca	ncel	Save		
			Co	pyright Kinsey 2015				

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

C espussiv:9090		
insey ESBus Home Pa 🦅 MSN.com		
kinsey	Logged in as:	admin
Transaction Auditing	ctivity Monitor LAUA Reporting LS Reporting SoD Reporting Analytics Administration	
Overview	ASSET MANAGEMENT CASH MANAGEMENT CLOSING HR INVENTORY MISC ORDER ENTRY PAYABLES PAYROLL RECEIVABLES	Â
Lawson IOS Controls	Add Naw B	ula
Scheduled Tasks	Fashed Importance Title/Comment	lie
Transaction Audit Rules Reporting Groups	2 @ 😭 🖄 🖄 🖄 10.11 Initiate Disposal of Fixed Assets conflicts with Reconcile Fixed Assets Subsidiary Ledger to General Ledger. One person should not have responsibility over both the access to assets and the responsibility for maintaining the accountability for such assets.	æ
SOD Rules Scheduled Reports	2 @ \$	ŧ
User Administration Administer Problematic Forms	get 2 2 get 2 2 2 get 2 2 2 get 2 2 2 get 2 2 2 get 2 2 2 get 2 2 2 get 2 2	æ
Metadata Editor Manage Restrictions	g g	æ
View Error Log	2 @ 含含含含念 11-14 Reconcile Fixed Assets Subsidiary Ledger to General Ledger conflicts with Edit Fixed Asset Master File. If one individual has responsibility for more than one of these functions, that individual could misappropriate assets and conceal the misappropriation.	æ
	2 @ (\$\overline\$) \$\overline\$) \$\overline\$ \$\overli	æ
	2 @ 含含含含合. 11 Initiate Purchase of Fixed Assets conflicts with Reconcile Fixed Assets Subsidiary Ledger to General Ledger. One person should not have responsibility over both the access to assets and the responsibility for maintaining the accountability for such asset	æ
	2 @ (\$	=
	2 @ 含含含含合. 07-14 Initiate Purchase of Fixed Assets conflicts with Edit Fixed Asset Master File. If one Individual has responsibility for more than one of these functions, that individual could misappropriate assets and conceal the misappropriation.	æ
	② 会会会会会会会会会会会会会会会会会会会会会会会会会会会会会会会会会会会会	:
	🖉 🤕 🛧 🛧 🛧 🛧 🔆 0.7.00 loisiate Durcharo of Event conflicts with Record Event Accest Transactions. One parent should not have reconnectability ours both the accest to	•

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.

What type of SOD Object is this?
Please select the type of object ARSUP is: Form Table* System Code* Role* Field* * These types of objects will only work with the Lawson Security 9 (or greater) security models. SOD Reporting for LAUA security will skip the above object types.
Submit Cancel

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.

🚖 Add a new rule						
Category:	ASSET MANAGEMENT	•				
Description:		1.				
Group operation:	AND (all items in group ORed together)	Ŧ				
Cancel	Save					

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.

Rule Importance				Title/Comment
	New HR Rule			
		Group ID: 0 [OR] HOLDER +	AND	ADD NEW GROUP

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.

← → C 🗋 esbussrv/		् 👷 🔳
🔛 Apps 📄 Kinsey ESBus Home Pa (MSN	Lan	
		Logged in as: m
Transaction Auditing	Activity Monitor LAUA Reporting LS9 Reporting SOD Reporting Administration	
Overview	Environment Setup	
Lawson IOS Controls Configuration	Basic Server Configuration	
Transaction Audit Rules	Transaction Auditing Global Configuration	
SOD Rules Scheduled Reports User Administration Administra Problematic Forms	Segregation of Duties Global Configuration SOD Function Code Violations (comma delimited): AC.D.Q. Role(a) to skip with SOD Reporting (comma delimited, LS9 ONLY): Use database for LS9 SOD (not LDAP): Secclass(es) to skip with SOD Reporting (comma delimited, LAUA ONLY):	
Manage Restrictions View Error Log	+ Temporary File Locations	
	LAUA Email Configuration (PROD Environment)	
	LAUA Email Configuration (TEST Environment)	
	Lawson Configuration (Production Server)	
	LID Server Configuration (Production Server)	
	ESS Tracking Application Configuration (Production Server)	
	LS9 Security Configuration (Production Server)	
	Active Directory (Prod Server)	
	Copyright 2000 - 2014	

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. <i>Line code function codes are not checked when looking for SOD violations.</i>
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.

Kinsey & Kinsey, Inc. Confidential 2008-2015 (v.0625)

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.

Deny Any Access Unconditional Access for Action	+,-J,N,P	Available Choices	
Conditional Rule Access Rule Type	If Then Else	 ✓ + - PageDown ✓ PageUp ✓ I - Inquire ✓ N - Next ✓ P - Previous 	2

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

Note: <u>For Kinsey's SoD application Inquiry-only</u> 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 <u>SOD Function Code Violations</u> 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.

🔥 • My Tasks in kinsey.com - 🗆 🗙 K Kins	sey Portal	×				J				
← → C ㎡ 🗅 esbussrv:9090)									ର୍ 🚖 🔳
🔛 Apps 🗽 Kinsey Portal 🚺 MSN.com 🤳	• Dan's kinsey.com 1	T K Advance SOD Reporting								C Other bookmarks
kinsey										
Transaction Auditing	Activit	y Monitor	AUA Reporting	LS Reportin	ng Landma	rk SoD Re	porting	Analytics	Administration	
Overview	Segregation	n of Duties Trans	saction Auditor	LS Reporting	LS Audit Report	ting Edit Grou	ps/Sched	ules LS Report	Snapshots Sent Re	ports
Configuration	Server ID	Name		Last Run	Schedule	Email Group	Action	Remove		
Scheduled Tasks	BOTH	Finance Dept Re	port 8	/1/2015 6:00 PM	End of Week	Finance	Enable	(B)		
Transaction Audit Rules	BOTH	fnelson security	11	/7/2015 6:00 PM	End of Week	Finance	Disable			
Reporting Groups	BOTH	Finance User Rol	e Report 11	/7/2015 6:00 PM	End of Week	Finance	Disable	•		
SOD Policies	BOTH	AP Roles	7/2	20/2015 9:59 AM	every minute	HR Admin	Enable			
Scheduled Reports	BOTH	Management Ta	sk 11/	7/2015 11:00 PM	dk	dk	Disable			
Problematic Forms	BOTH	Acbudgets	11/	7/2015 11:00 PM	dk	dk	Disable	•		
Metadata Editor										
Manage Restrictions										
View Error Log										
4					Copyright Kins	ey 2015		_		

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.

Report email group	1
Name: Finance	
Send to email address(es):	
d.kinsey@kinsey.com	
	/
	Carro
	Save



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.

Schedu	le: End of V	Veek						
Name:	End of W	'eek						
Every	week	on	Saturday	at	18):[00	
	minute	- 1						
	hour	- 1	Sa	ve				
	day	- 1						
	week							
	month							
	year	- 1						
	-	_						

Reports using: End of Week
LS9 Audit Reporting Change made by Lawson
SOD Reporting • AP Policies • Critical Financial Policies
Transaction Audit Reporting • Accounting Units • Activity • AP Invoice AP30.1 • AP Setup • baylor • Customer Terms

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

Kinsey & Kinsey, Inc. Confidential 2008-2015 (v.0625)

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.

isey ESBus Home Pa 🚺 MSN.com												
kinsey [*]											Logge	d in as: admi
Transaction Auditing	Activity M	onitor LAUA Report	ing LS	Reporting	SoD Re	porting	Analytics	Administ	tration			
Overview											A	dd New User
Lawson IOS Controls Scheduled Tasks	Usernam	e Email	ESBus Admin	TA Reports	SOD Reports	AM Reports	LAUA Analyzer	LS Reports	LAUA Audit	LS Audit	Last Modified	
Transaction Audit Rules	admin	admin@kinsey.com		۲			۲				2/10/2015 10:42AM	▼ 🗾 🗄
Reporting Groups	bill	bill@domain.com									2/10/2015 10:53AM	🔻 🗾 🔁
SOD Rules	mike	mike@domain.com					•				2/10/2015 10:53AM	v 🗾
Scheduled Reports	mnitka	mnitka@domain.com		1		•	•		•	•	2/10/2015 10:53AM	V
User Administration											2, 10, 2010 10:000	-
Administer Problematic For	ms											
Mapage Postrictions												
View Error Log												
VIEW EITOI LOB												

To set up a new User select the Add New User button.

🚖 Create new user	×
Username	
Password	
Confirm Password	
Email Address	
Cancel	Create

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.

Username	e Email		ESBus Admin	TA Reports	SOD Reports	AM Report	LAI s Anal	UA lyzer R	LS eports	LAUA Audit	LS Audit	Last	Modified		
admin	admin@kin	sey.com					•					6/22/2015	9:13AM		/
Admini	stration	IOS 💽	Config 💌	Scheduled Tasks 🕑	Audit Rules 🕑	Report Groups	SOD Rules	Schedule Reports	d User Admin 🖌	Problem Forms	Metadata Editor 🕑	Manage V Restrictions	liew Error Log ✔		
Transa	ction Reports	Export 🗹	Report Restrictions												
Activity	Monitor	Excel Results													
LS Repo	orts	Security Reports	Security Analyzer 🕑	Form Modeling	Role Modeling Co	Object omparison \ 🕑	Security Visualizer	Security Utilities							
		•													
bill	bill@domai	n.com			•	•						6/19/2015	12:54PM	-	2 🔁
mike	mike@dom	ain.com										2/10/2015	12:54PM	-	<u>/</u>
mnitka	mnitka@do	main.com	e	1			4				1	3/25/2015	2:31PM	•	2 🔁

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.

ports - Restrictions	×
separated by semicolons (";")	
LINEDTL-TABr0	
separated by semicolons (";")	2
	Save
	ports - Restrictions

Changing or Deleting a User

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

											to an address	
спѕеу											Logged in	as: admi
Transaction Auditing	Activity M	onitor LAUA Report	ing LS	Reporting	SoD Re	eporting	Analytics	Adminis	tration			
Overview											Add N	lew User
Lawson IOS Controls Scheduled Tasks	Usernam	e Email	ESBus Admin	TA Reports	SOD Reports	AM Reports	LAUA Analyzer	LS Reports	LAUA Audit	LS Audit	Last Modified	
Transaction Audit Rules	admin	admin@kinsey.com				•					2/10/2015 10:42AM 🔻	1
Reporting Groups	bill	bill@domain.com				•					2/10/2015 10:53AM 🔻	🖍 🕀
SOD Rules	mike	mike@domain.com					•				2/10/2015 10:53AM 🔻	🗾 🕀
Scheduled Reports	mnitka	mnitka@domain.com	•	•	•	•	•	•	•	•	2/10/2015 10:53AM 🔻	
Administer Problematic For	ms											
Metadata Editor												
Manage Restrictions												
View Error Log												

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.

📕 Update passwo	ord	×
Username	admin	
Password		
Confirm Password		
Email Address	admin@kinsey.com	
Cancel		Update

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.

🗅 Kinsey Portal 🗙 📃		
← → C f ⊡ esbussrv:9090		् 🚖 🗉
🔛 Apps 🗋 Kinsey Portal 🚺 MSN.com		Other bookmarks
kinsey	Logged in as: admin (+	A
Transaction Auditing Activity Monitor	LAUA Reporting LS Reporting SoD Reporting Analytics Administration	
Overview	Reason Form Name Form Description Added By When Added	^
Lawson IOS Controls	+ GL20.2 Posting Accounts admin 2/3/2014 11:11 AM	
Configuration		
Scheduled Tasks	+ PR85.2 Bank Account Totals admin 5/2/2013 1:01 PM	
Transaction Audit Rules		
Reporting Groups		
SOD Policies	Token:	
Scheduled Reports	Reason (optional):	
User Administration		
Problematic Forms		
Metadata Editor		
Manage Restrictions	Add Joken	
View Error Log	Add Token	
		-
	Copyright Kinsey 2015	

View Error Log

insey Portal 🚺 MSN.com								<u> </u>	
kinsey							Logge	ed in as: admin 🔆 清	
Transaction Auditing	g Acti	vity Monitor	LAUA Reporting	LS Reporting	SoD Reporting	Analytics	Administration		
Overview	Display la	ast: 500 🔹						<u>Clear Log</u>	
Lawson IOS Controls	Details	Date	Erro	r Message					
Configuration	+	4/5/2015 11	:42 AM Asse	ssmentFilter (doFil	ter) ROUTER TRANS	ACTION ERROR	R:For input string:	"***"	
Scheduled Tasks	-	4/5/2015 11	:42 AM Asse	ssmentFilter (doFil	ter) ROUTER TRANS	ACTION ERROR	EFor input string:	"***"	
Transaction Audit Rules	· · ·	1,0,201011					and input string.		
Reporting Groups	java.i at iav	ang.NumberFor a.lang.NumberF	ormatException: For	nput string: rInputString(Number	FormatException.iava:	59)			
SOD Policies	at jav	a.lang.Integer.p	arseInt(Integer.java	:460)	,,	,			
Scheduled Reports	at jav	a.lang.Integer.p	arseInt(Integer.java	:510)					
User Administration	at cor	n.kinsey.Assess	ment.AssessmentFi	Iter.doFilter(Assessm InstancoWrappor.do	entFilter.java:/86) Filtor/FiltorInstancoWr	appor java:190)			
Drahlamatia Forma	at cor	n.ibm.ws.webc	ontainer.filter.Web	AppFilterChain.doFilt	er(WebAppFilterChain	.java:125)			
Problematic Forms	at cor	m.lawson.servle	t.AuthenticationFilt	er.doFilter(Authentio	ationFilter.java:105)				
ivietadata Editor	at cor	n.ibm.ws.webco	ontainer.filter.Filter	InstanceWrapper.do	Filter(FilterInstanceWr	apper.java:190)			
Manage Restrictions	at cor	n.lawson.servle	t.CallLoggingFilter.o	loFilter(CallLoggingFi	lter.iava:117)	.Java.123)			
View Error Log	at cor	n.ibm.ws.webco	ontainer.filter.Filter	InstanceWrapper.do	Filter(FilterInstanceWr	apper.java:190)			
	at cor	n.ibm.ws.webc	ontainer.filter.Web	AppFilterChain.doFilt	er(WebAppFilterChain	.java:125)			
	at com.lawson.serviet.XSSValidatorFilter.doFilter(ASSValidatorFilter/Java:112)								
	at com.ibm.ws.webcontainer.filter.WebAppFilterChain.doFilter(WebAppFilterChain.java.126)								
	at com.ibm.ws.webcontainer.filter.WebAppFilterChaindoFilter(WebAppFilterChain.java:80)								
	at com.ibm.ws.webcontainer.filter.WebAppFilterManager.doFilter(WebAppFilterManager.java:908)								
	at com.ibm.ws.webcontainer.servlet.ServletWrapper.handleRequest(ServletWrapper.java:935) at com ibm.ws.webcontainer.servlet.ServletWrapper.handleRequest(ServletWrapper.java:932)								
	at cor	n.ibm.ws.webco n.ibm.ws.webco	ontainer.servlet.Ser	vletWrapperImpl.har	idleRequest(ServletWi	rapperImpl.java	:181)		
	40.001								

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 > <u>com.esbus.appliance.ls9</u> 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 > <u>com.esbus.appliance.serverUtil.GetLawsonListuserMap_TimerTask</u> 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. <u>If a connection cannot be made, Lawson's</u> <u>Portal application will not respond correctly</u>.

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:

 $J5.6.20t > \Psi\%h`*K{M \oplus C}#_75D6"FwG=<mysql_native_password$

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: