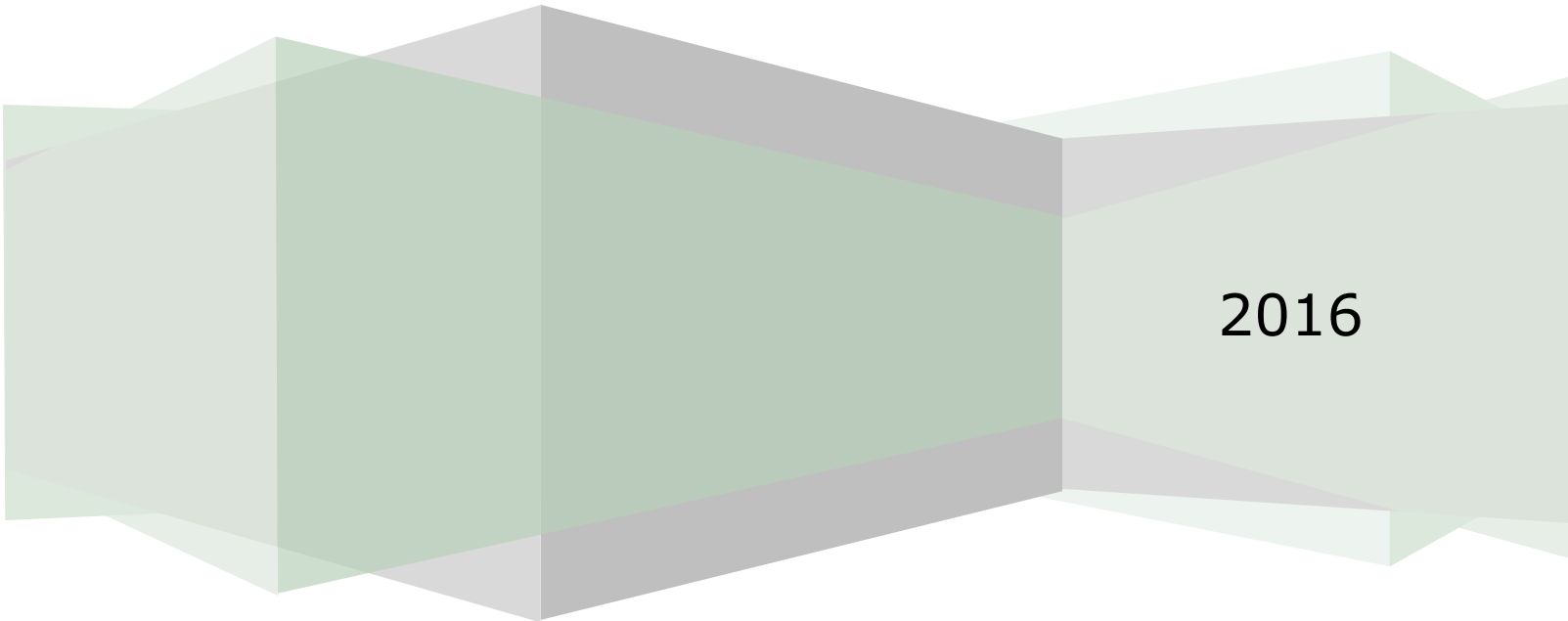




Landmark Security Reporting User Guide

A decorative graphic at the bottom of the page consists of several overlapping, semi-transparent geometric shapes in shades of green and grey, creating a layered, architectural effect.

2016

Contents

Introduction3

Logging in4

Landmark Security Reports5

 Pre-Report Filters7

 Adding or Removing Selected Values.....9

 Adding or Dropping All Values 10

 Adding or Removing Criteria Based Filters..... 11

 Historical Comparisons 12

 Changing Pre-Report Filters 13

Showing and Hiding Columns 13

On-The-Fly Report Filters 14

Grouping 15

 Creating a Group 15

 Grouping - Nested 17

 Grouping – Expand, Collapse or Remove 17

 Grouping – Remove Filters..... 18

Sorting..... 18

 Adding a Sort Option..... 18

 Removing the Sort Option..... 19

Saving Reports..... 19

 Saving New Security Reports 19

 Changing and Saving an Existing Report..... 20

Running Saved Report 20

Exporting and Printing..... 20

Drilling 21

Historical Reports 23

Scheduling Security Reports 23

Deleting a Report 24

Trouble Shooting..... 25

Introduction

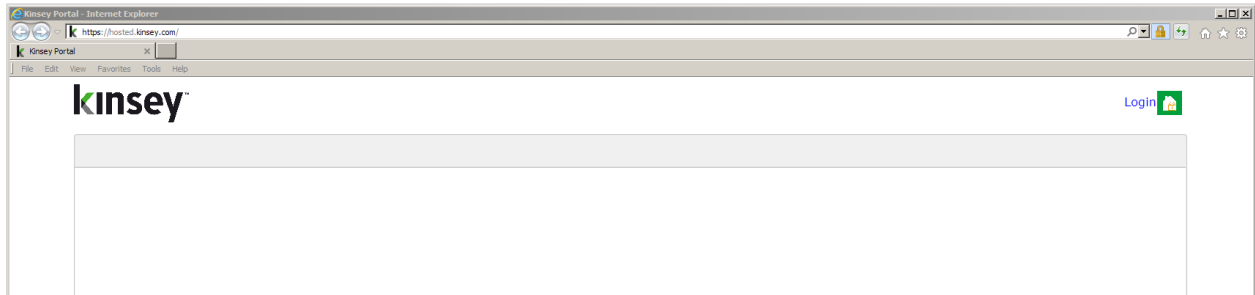
The Kinsey Landmark Security Reporting provides user friendly security reports, historical security reports and security change reports.

The security reports are designed to help with the administration of Landmark Security. They include detailed security information by Actor, Role and Security Class including all objects and rules.

These queries have been designed to provide access to your data in the quickest most robust method possible through a browser interface. The Security reports provide critical insight into your security model for your security administrators and your security auditors.

Logging in

To access your reports you must first login in the Security Dashboard. Click on the **Login** link in the top right corner of the Dashboard page.



Enter the user name and password.

Kinsey Portal Login

User

Password

Login

[Go back to homepage](#)

[Reset password](#)

To change your password select the Reset password link at the bottom of the login screen.

Password Reset

Email address:

I'm not a robot

reCAPTCHA
Privacy - Terms

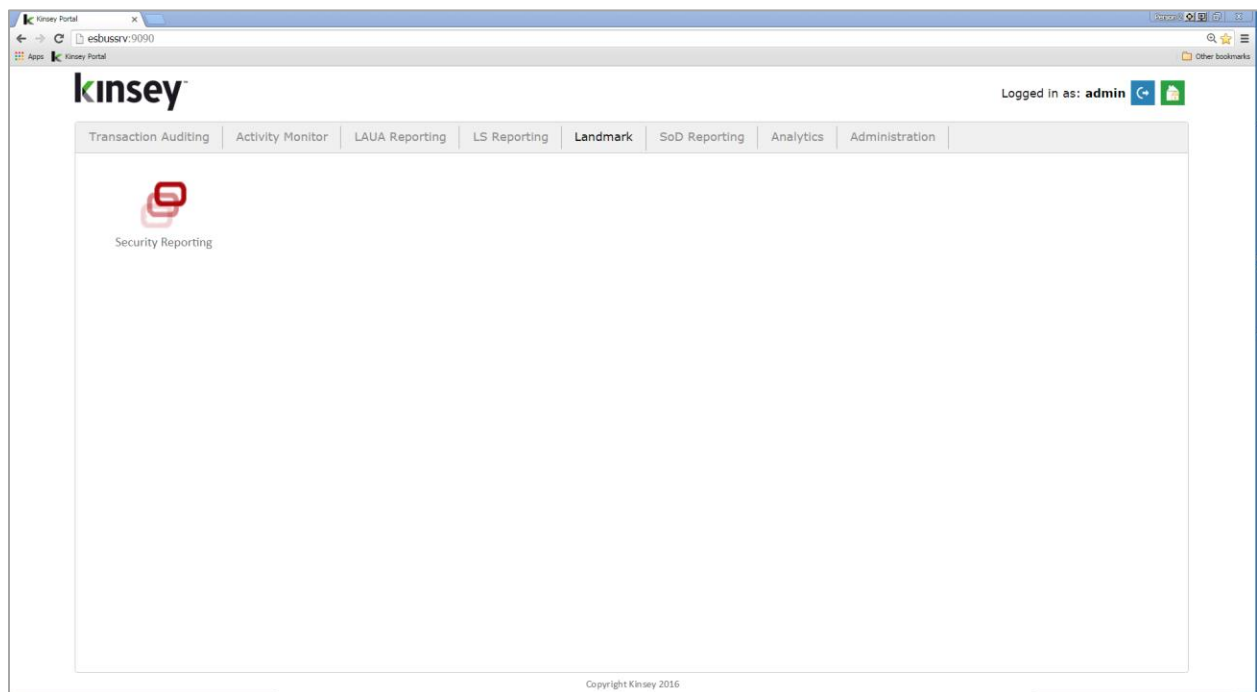
Reset Password

Once you enter you email address you will receive instructions on how to reset your password.

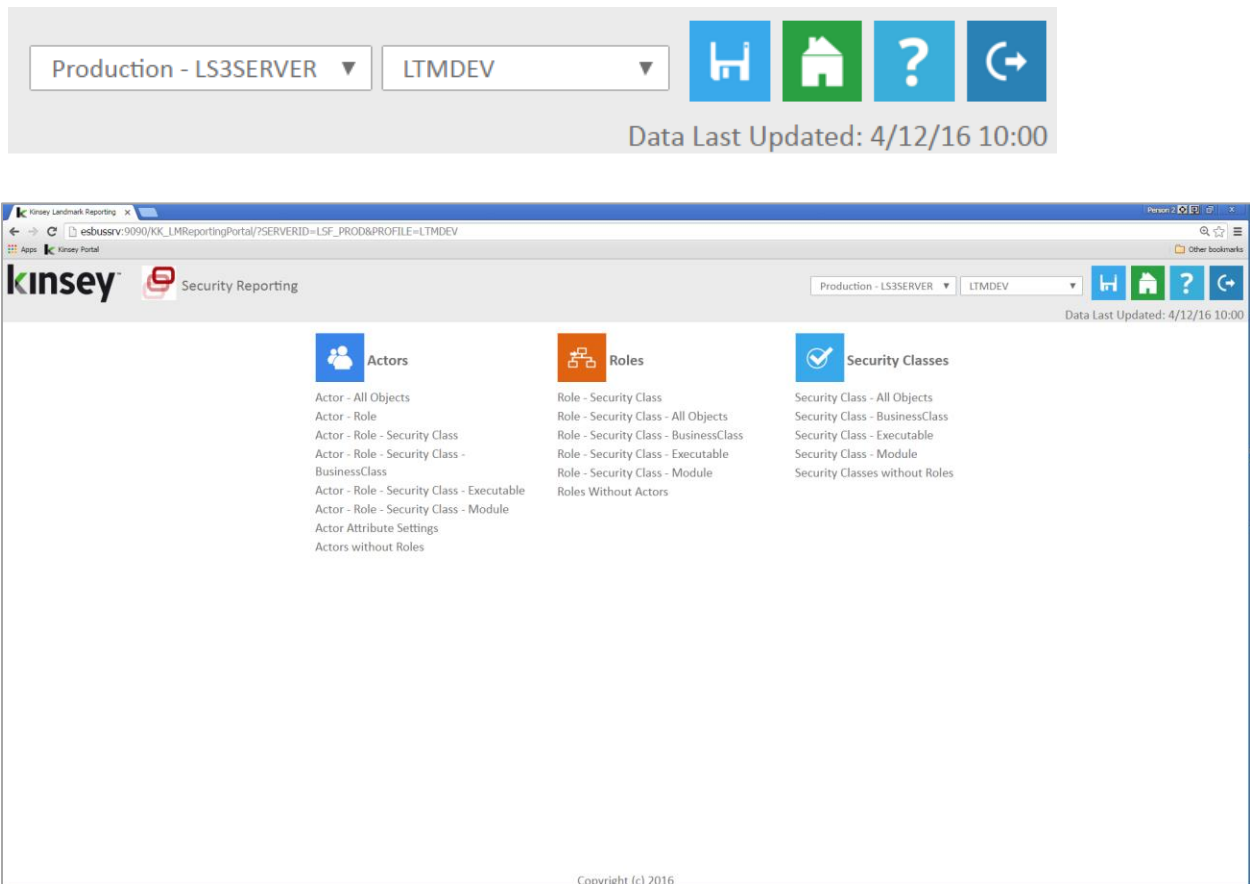
Landmark Security Reports

The Landmark Security reports are designed specifically for anyone that needs to maintain security for the Landmark applications. Although these reports can be used by the auditors, they provide more insight into the technical aspects of the model that is not generally required by an auditor.

Launch the Security Dashboard and select the Security Reporting icon from the Landmark Reporting tab.



Start by selecting the server and profile you want to report on in the top right corner of the screen. You can select to view reports based on current settings or historical snapshots (Advanced version only). Historical snapshots can be created through the administration panel. Refer to the Kinsey Administrator Guide, page 12, Schedule Tasks for more information.



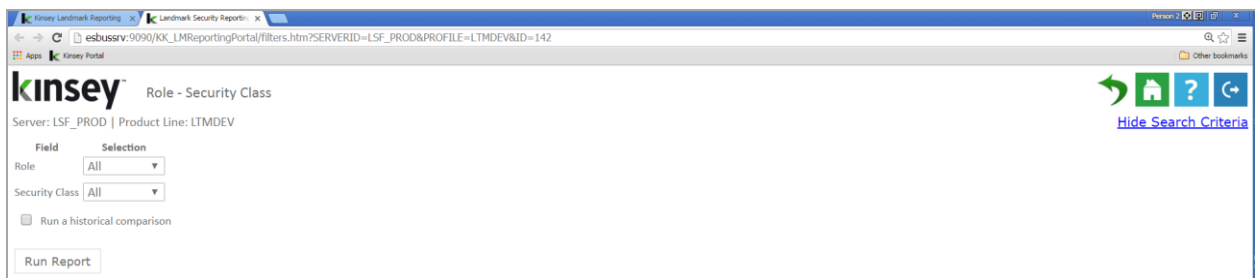
The Security Reporting dashboard comes preconfigured with reports for Actors, Roles and Security Classes.

Report Features

Pre-Report Filters

The report filters allow you to restrict the amount of information that will be retrieved from the database prior to generating the report. This is helpful when you are working with a large amount of data and only want a small subsection to analyze.

All of the report filters follow the same convention. The filter options will vary depending on report selected.



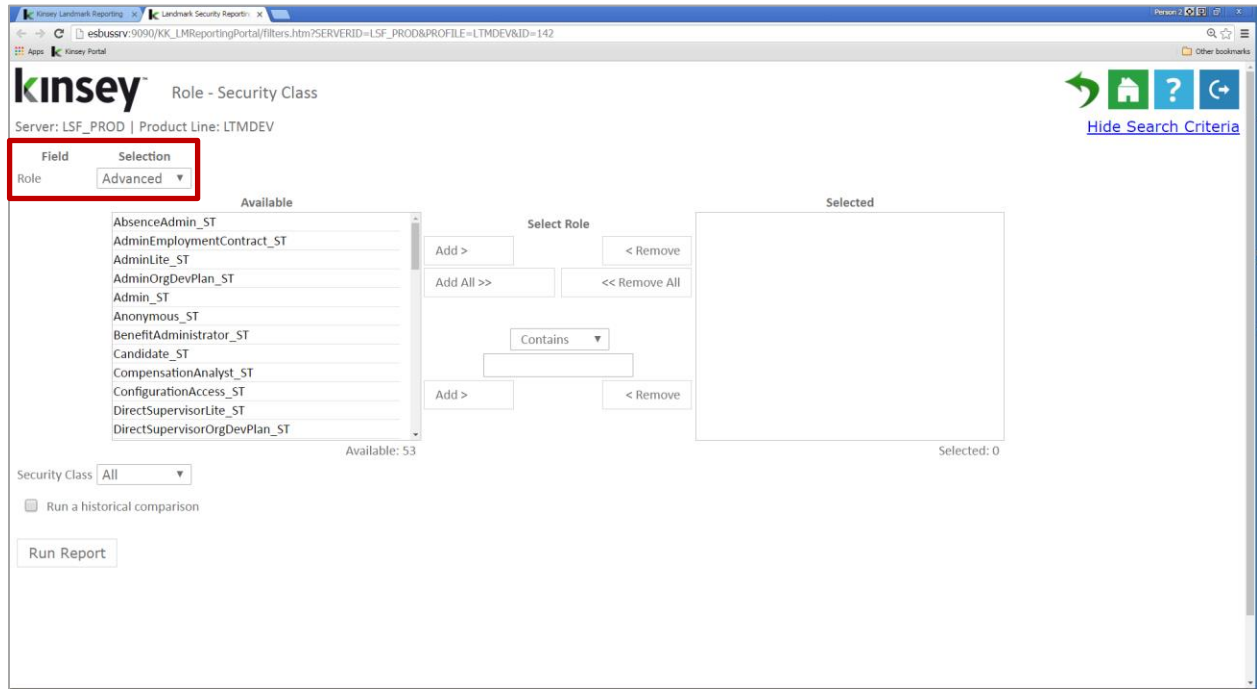
For example, on the Role – Security Class report you will have the option of filtering by Role or Security Class. If you need to filter by any other field you can do that once the grid is populated. All filters assume “AND” logic, meaning all values must satisfy the criteria for data to be displayed.

There are 2 methods when using filters. The first simply provides the option of selecting the condition and filling in the value. For example, in the above example to report on a specific Role you would simply change the “Selection” value to “Equals” and fill in the appropriate value. Repeat the process for the Security Class field. If you want the application to return all values for a field you do not need to make a selection.

Filter Expressions

Equals	Value entered must match data exactly.
Contains	Value entered must be contained within the data.
Starts With	Data returned must start with value entered.
Ends With	Data returned must end with the value entered.
Is Between	Date returned must fit within the range selected.
Regular-Ex	Similar to OR logic. Entered as value value value etc.

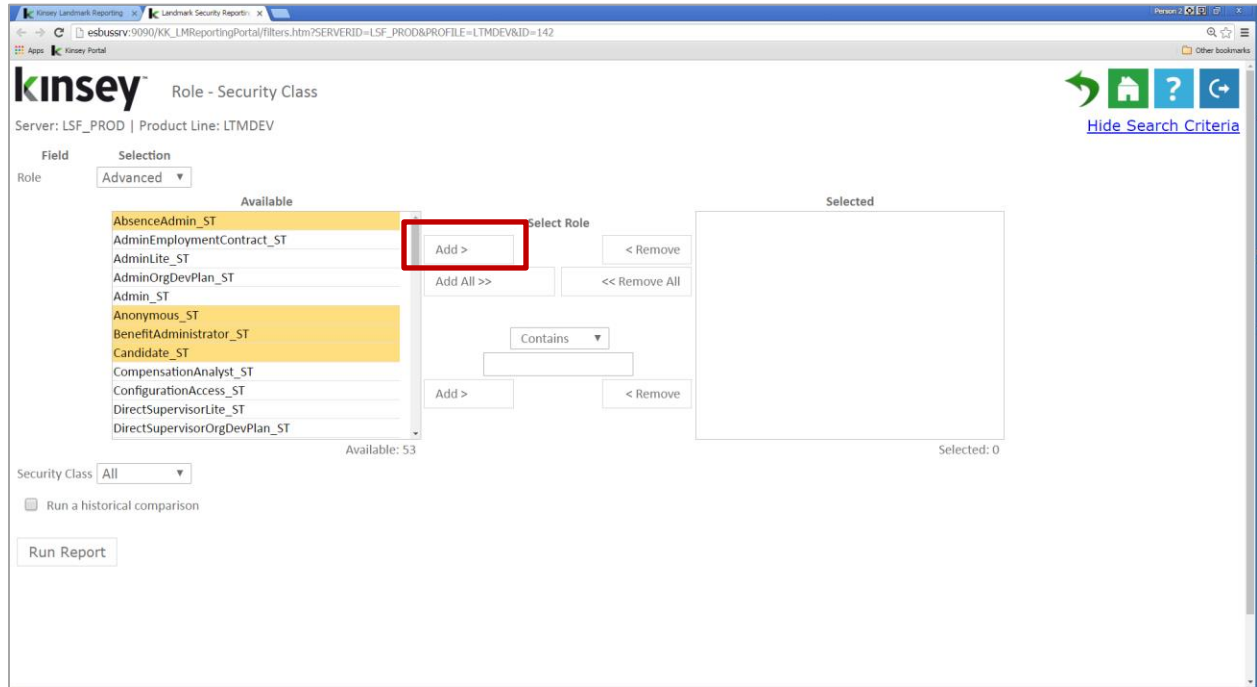
The second method allows you to select from a list of possible values. This option can take a little time to populate depending on the size of your model. The values shown are based on the information available in the model.



Start by selecting "Advanced" as the condition. The application will display all of the available values associated with the specific field. For instance, in the example above all of the Roles are displayed in the Available column. At this point you have a couple of ways to select the Roles you would like included on the report.

Adding or Removing Selected Values

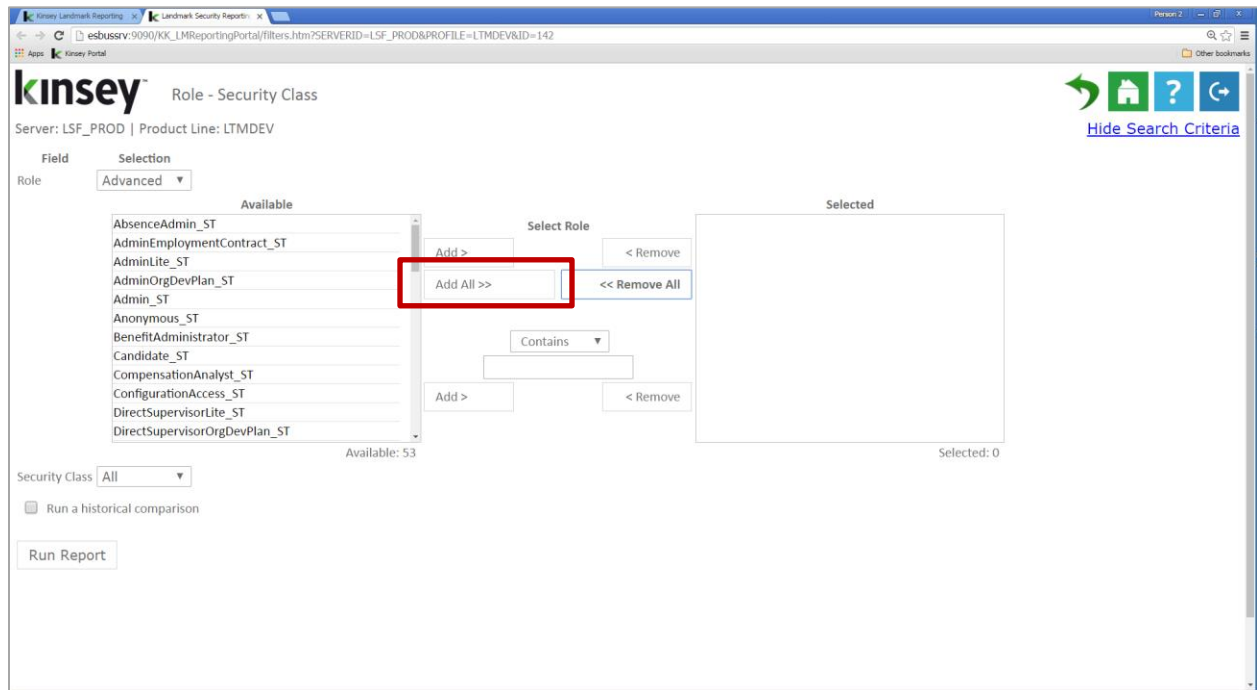
While holding down the CTRL key click on the Roles you want added to the report then click on the drop **Add >** button. To remove a values from the list select the items in the 'Selected' column and click on **< Remove**.



Adding or Dropping All Values

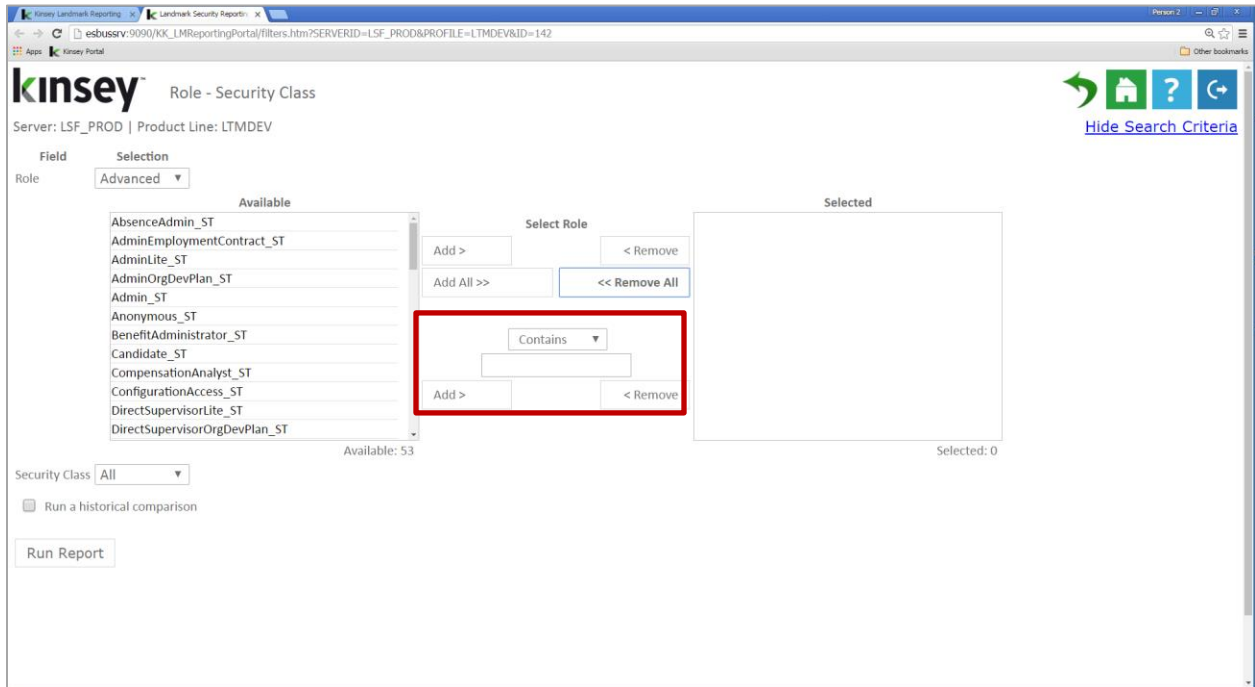
To add all Roles simply click on the **Add All >>** button. To remove all select the **<< Remove All** button.

Tip: There may be time where it's easier to add all and then remove the values you don't want selected rather than selecting a large list for inclusion.



Adding or Removing Criteria Based Filters

To add Roles based on specific criteria you can use the condition option to make your selection. Start by selecting the condition.



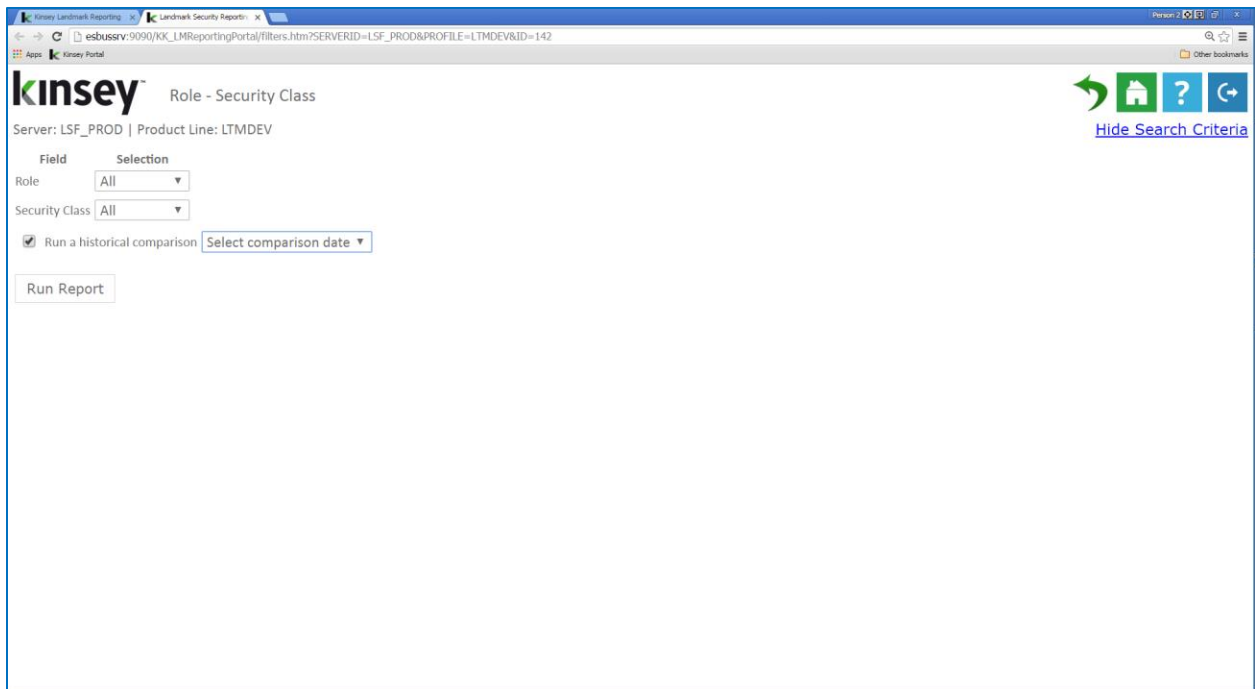
There are 2 options on which you base your logic; Contains and Starts With. In this example I will select "Contains", enter the value of "manager" and select the **Add >** button. As you can see all of the Roles containing "manager" in their ID or name have been moved to the selected list. You can remove items from the Selected list by entering a condition and selecting the **< Remove** button.

Tip: In all cases you can Add or Remove by combining the methods or repeating a method as needed. For example you could Add all values starting with "ACCT" and then also Add all values containing "super".

Historical Comparisons

When you run a historical comparison (only available with the advanced reporting version) the application will ONLY return the changes between the current security model and the baseline you are comparing to. This should not be considered a true change audit report but rather a differences report from the last approved security review.

After you have selected the appropriate filters check the 'Run a historical comparison' field. The application will prompt you for the time stamped database you would like compared. If no comparison dates are available see your system administrator about creating a baseline snapshot.

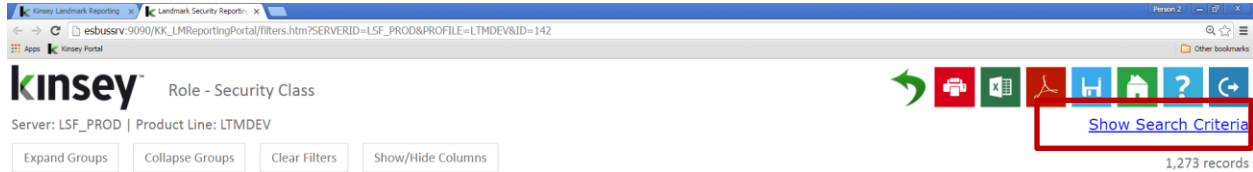


The screenshot shows a web browser window displaying the Kinsey Security Dashboard. The page title is "Role - Security Class". The server information is "Server: LSF_PROD | Product Line: LTMDEV". There are navigation icons (back, home, help, forward) and a "Hide Search Criteria" link. The main content area has a table with two columns: "Field" and "Selection". The "Role" field has a dropdown menu set to "All". The "Security Class" field has a dropdown menu set to "All". Below the table, there is a checkbox labeled "Run a historical comparison" which is checked, and a dropdown menu labeled "Select comparison date". A "Run Report" button is located below the checkbox.

Note: You cannot run a historical comparison if you have selected a historical database for reporting. This option will be hidden when running historical reports.

Changing Pre-Report Filters

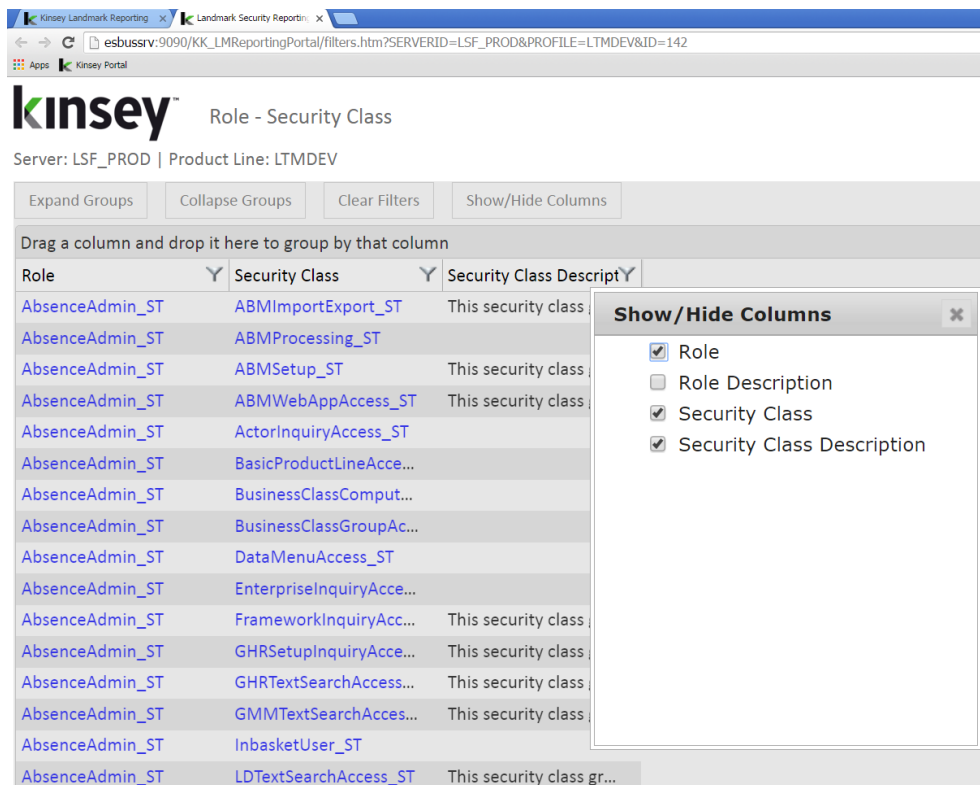
To change your selection criteria without exiting the report simply select the Show Search Criteria link in the upper right corner of your screen..



Showing and Hiding Columns

The report screen will allow you to change the columns displayed once the grid is populated. The application will default to the settings found under the LS Security Configuration option on the Administrative Configuration page.

Select the Show/Hide Columns button to select the columns you want displayed.



On-The-Fly Report Filters

You can also filter your results once the grid has been populated. Select the filter icon next to the field name in the header.

The screenshot shows a web browser window displaying the Kinsey Security Dashboard. The page title is "Role - Security Class - BusinessClass". The URL is "esbussrv:9090/KK_LMReportingPortal/filters.htm?SERVERID=LSF_PROD&PROFILE=LTMDEV&ID=148". The page shows a table with 14,827 records. The table has the following columns: Role, Security Class, Type, Object, and Rule. The 'Object' column header has a filter icon (a small 'Y' in a square) circled in red. The table contains 15 rows of data, each representing a different security class and its associated objects and rules.

Role	Security Class	Type	Object	Rule
AbsenceAdmin_ST	ABMImportExport_ST	BusinessClass	EmployeeBalanceExport	is accessible for all actions unconditionally
AbsenceAdmin_ST	ABMImportExport_ST	BusinessClass	GeneralLedgerExport	is accessible for all actions unconditionally
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	LeaveOfAbsence	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	TemporaryGeneralLedgerPosting	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	EmployeeTransactionSummary	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	TimeOffRequest	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	TemporaryEmployeeAbsencePlanDates	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	EmployeeAbsenceTransaction	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	EmployeeAbsenceHoursAllocation	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	EmployeeLengthOfServiceHours	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	TemporaryEmployeeAbsencePlanUpdate	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	TemporaryEmployeeAbsencePlanCreate	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	TemporaryEmployeeAbsencePlanTransfe...	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	TemporaryLeaveOfAbsenceRestore	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	TemporaryEmployeeHoursAllocation	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	EmployeeHoursAllocationDetail	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	EmployeeAbsencePlan...	is accessible for all actions when (Employee.IsNotEmployee) is access

Copyright (c) 2016

A↓ Sort Ascending

 Z↓ Sort Descending

 A Z× Remove Sort

 Group By this column

 Remove from groups

 Show rows where:

 contains

 And

 contains

 Filter Clear

Each column as has the option to add on-the-fly filters. When you select the filter icon next to the column header you will see the option "Show rows where:". To add a filter simply select the condition and enter the value. The conditions include; contains, empty, not empty, contains (match case), does not contain, does not contain (match case), ends with, ends with (match case), equals, equals (match case), null, not null. You can nest up to 2 conditions using either AND or OR logic. To change to OR login select the down arrow next the word 'And' and change the option to 'OR'.

Grouping

Creating a Group

The grouping option provides a dynamic way of viewing your data in a summarized format without having to generate a new query. This option can turn a single query into multiple dimensions.

Let's take a look at the following query for Role – Security Class – Business Class

Kinsey Landmark Reporting - Landmark Security Reportin...

 esbussrv:9090/KK_LMRReportingPortal/filters.htm?SERVERID=LSF_PROD&PROFILE=LTMDEV&ID=148

 Kinsey Portal

kinsey Role - Security Class - BusinessClass

 Server: LSF_PROD | Product Line: LTMDEV

 Expand Groups Collapse Groups Clear Filters Show/Hide Columns

 Show Search Criteria

 14,827 records

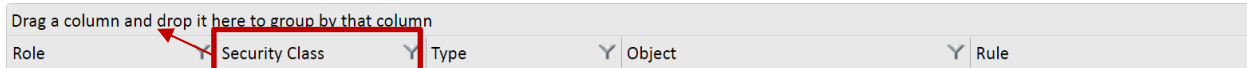
 Drag a column and drop it here to group by that column

Role	Security Class	Type	Object	Rule
AbsenceAdmin_ST	ABMImportExport_ST	BusinessClass	EmployeeBalanceExport	is accessible for all actions unconditionally
AbsenceAdmin_ST	ABMImportExport_ST	BusinessClass	GeneralLedgerExport	is accessible for all actions unconditionally
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	LeaveOfAbsence	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	TemporaryGeneralLedgerPosting	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	EmployeeTransactionSummary	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	TimeOffRequest	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	TemporaryEmployeeAbsencePlanDates	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	EmployeeAbsenceTransaction	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	EmployeeAbsenceHoursAllocation	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	EmployeeLengthOfServiceHours	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	TemporaryEmployeeAbsencePlanUpdate	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	TemporaryEmployeeAbsencePlanCreate	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	TemporaryEmployeeAbsencePlanTransfe...	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	TemporaryLeaveOfAbsenceRestore	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	TemporaryEmployeeHoursAllocation	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	EmployeeHoursAllocationDetail	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	EmployeeAbsencePlanDe...	is accessible for all actions when (Employee.IsNotEmployee) is access

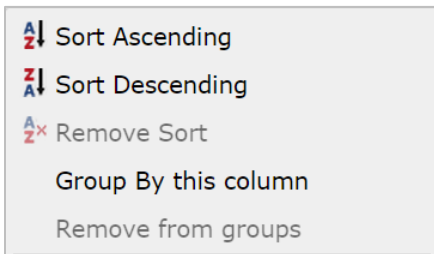
 Copyright (c) 2016

By default the query is going to be displayed in detail by Role, Security Class and Business Class. But let's say we want to rearrange the list and group it by Security Class to see all of Roles assigned to each Class.

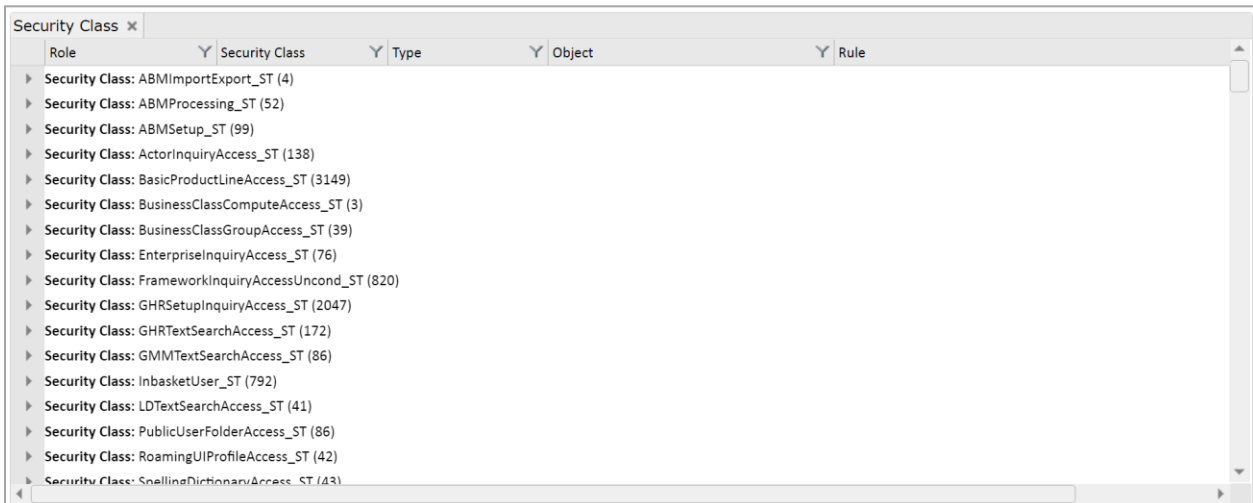
Start by dragging the 'Security Class' column header to the open area on the title bar. The header will display with a green check mark once it's in the proper position.



Alternatively you can select the drop down arrow next to the column title and choose Group by this column.



The grid will be redisplayed and grouped by Form.



You can now see the number of assignments for any specific Security Class. To see those assignments click on the arrow left of the Security Class name.

Role	Security Class	Type	Object	Rule
	Security Class: ABMImportExport_ST (4)			
	Security Class: ABMProcessing_ST (52)			
	Security Class: ABMSetup_ST (99)			
	Security Class: ActorInquiryAccess_ST (138)			
	Security Class: BasicProductLineAccess_ST (3149)			
	Security Class: BusinessClassComputeAccess_ST (3)			
AbsenceAdmin_ST	BusinessClassComput...	BusinessClass	Compute	is accessible for all actions unconditionally
AbsenceAdmin_ST	BusinessClassComput...	BusinessClass	BusinessSubject	is accessible for all inquiries unconditionally
AbsenceAdmin_ST	BusinessClassComput...	BusinessClass	ComputeSubject	is accessible for all actions unconditionally
	Security Class: BusinessClassGroupAccess_ST (39)			
	Security Class: EnterpriseInquiryAccess_ST (76)			
	Security Class: FrameworkInquiryAccessUncond_ST (820)			

The grid now displays the Roles, Security Class and Rule associated with the Business Class.

Grouping - Nested

Grouping can be done using multiple fields. See 'Grouping' to add your first group. Once this is complete you can add a second level by simply dragging another header to the title bar. In this example we will add Object to the Group.

Role	Security Class	Type	Object	Rule
	Security Class: ABMImportExport_ST (2)			
	Security Class: ABMProcessing_ST (26)			
	Security Class: ABMSetup_ST (33)			
	Security Class: ActorInquiryAccess_ST (2)			
	Security Class: BasicProductLineAccess_ST (67)			
	Security Class: BusinessClassComputeAccess_ST (3)			
	Object: Compute (1)			
	Object: BusinessSubject (1)			
	Object: ComputeSubject (1)			
	Security Class: BusinessClassGroupAccess_ST (3)			
	Security Class: EnterpriseInquiryAccess_ST (2)			
	Security Class: FrameworkInquiryAccessUncond_ST (20)			

As you can see the system will now report on the number of Security Class the Business Class can be found in. You can view the Roles assigned by expanding the list using the arrow left of Object.

Grouping – Expand, Collapse or Remove

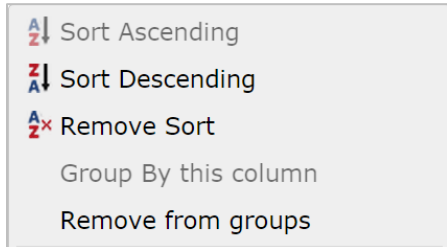
At the top of each report are additional options you can use when Grouping is performed.

Expand Groups
Collapse Groups
Clear Filters
Show/Hide Columns

Security Class
▾
Object
▾

Simply select the Expand or Collapse buttons to display or hide the grouping details. To remove a group entirely select the 'x' next to the title on in the header.

Alternatively you can select the filter icon next to the column title and choose Remove from Groups.



Grouping – Remove Filters

Any filter added to a column is maintained when Groups are used. To remove column filters select the Remove Filters button. The Groups will be maintained but the column filters will be removed.

Note: This does not affect the 'pre-report' filters created prior to generating the query.

Sorting

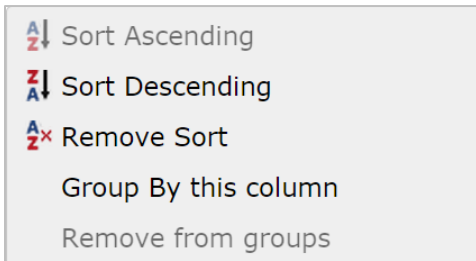
Adding a Sort Option

There are a couple of ways to sort the rows once the grip is displayed. The simplest method is to just click on the column Title.

Drag a column and drop it here to group by this column

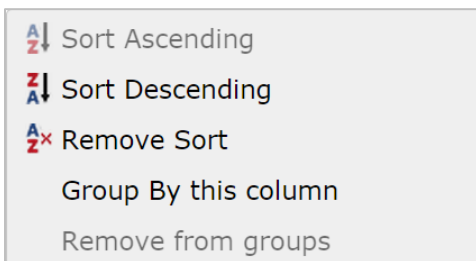
Role	Security Class	Type	Object	Rule
DirectSupervisor_ST	ABMDirectSupervisor...	BusinessClass	EmployeeAbsencePlan	is accessible for all inquiries when (Employee.AncestorDirectSupervis
DirectSupervisor_ST	ABMDirectSupervisor...	BusinessClass	AbsencePlanStructure	is accessible for all inquiries unconditionally
DirectSupervisor_ST	ABMDirectSupervisor...	BusinessClass	TimeOffRequest	is accessible for UpdateTimeOffByManager, RequestTimeOffByManag
DirectSupervisor_ST	ABMDirectSupervisor...	BusinessClass	AbsenceConfiguration	is accessible for all inquiries unconditionally
DirectSupervisor_ST	ABMDirectSupervisor...	BusinessClass	EmployeeAbsenceTransaction	is accessible for all inquiries when (Employee.AncestorDirectSupervis
DirectSupervisor_ST	ABMDirectSupervisor...	BusinessClass	AbsencePlanStructureOption	is accessible for all inquiries unconditionally
Employee_ST	ABMEmployee_ST	BusinessClass	AbsencePlanStructure	is accessible for all inquiries unconditionally
Employee_ST	ABMEmployee_ST	BusinessClass	AbsencePlanStructureOption	is accessible for all inquiries unconditionally
Employee_ST	ABMEmployee_ST	BusinessClass	TimeOffRequest	is accessible for RequestTimeOffByEmployee, all inquiries, UpdateTin
Employee_ST	ABMEmployee_ST	BusinessClass	AbsenceConfiguration	is accessible for all inquiries unconditionally
Employee_ST	ABMEmployee_ST	BusinessClass	Employee	is accessible for RequestTimeOffByEmployee when (IsEmployee)
Employee_ST	ABMEmployee_ST	BusinessClass	EmployeeAbsenceTransaction	is accessible for all inquiries when (Employee.IsEmployee)
Employee_ST	ABMEmployee_ST	BusinessClass	EmployeeAbsencePlan	is accessible for all inquiries when (Employee.IsEmployee)
AbsenceAdmin_ST	ABMImportExport_ST	BusinessClass	GeneralLedgerExport	is accessible for all actions unconditionally
AbsenceAdmin_ST	ABMImportExport_ST	BusinessClass	EmployeeBalanceExport	is accessible for all actions unconditionally

You can also select the arrow next to the column header and choose to sort in Ascending or Descending sequence.



Removing the Sort Option

Select the filter button next to the column header and choose 'Remove Sort'

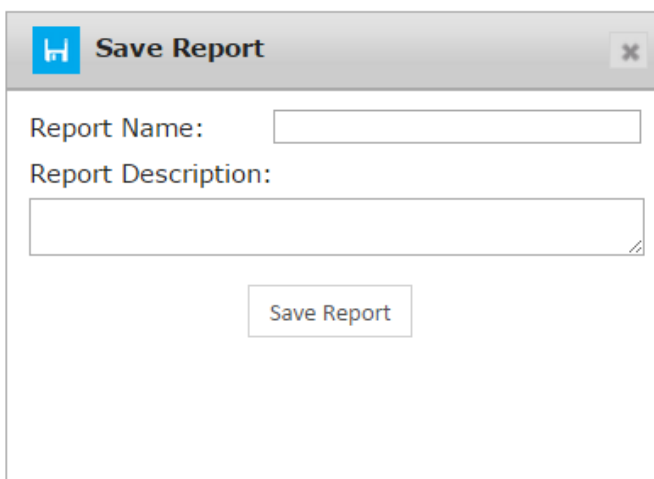


Saving Reports

Saving New Security Reports

You can save a report (only available in the advanced reporting version) by selecting the save icon once the report has been displayed on the screen. The application saves the search criteria and not the actual results of the query. Each time you run the report the application will use the saved filters to generate a new report.

Note: Saving a report does not save the sort sequence, grouping, column filters or historical flag that may have set prior to saving the report.



A dialog box titled 'Save Report' with a blue icon and a close button. It contains two input fields: 'Report Name:' with a text box and 'Report Description:' with a larger text area. A 'Save Report' button is centered at the bottom.

Changing and Saving an Existing Report

To save an existing report simply select the Save icon in the top right corner of the screen. You can save changes to an existing report by selecting the Overwrite existing option. To create a new report from a copy of an existing report select the New option and enter a new report name.

Running Saved Report

All saved reports are displayed as a row on the saved reports query. From the Security Reporting Home Page select the Save icon at the top of the screen. A list of saved reports will be displayed. Click on the Report Name to Run, Schedule or Delete the report.

Exporting and Printing

You can export or print your final query to Microsoft Excel , PDF of HTML once you have set all of your parameters by clicking on the appropriate icon at the top of the page. Limited export options are available in the Standard version.



The MS Excel export will maintain the grouping, sorting, columns and filters you have created in the query, but the column widths will need to be adjusted once you are in Excel.

Is the example below the query was grouped by Role prior to the export. To view the Role detail form within Excel click on the '+' sign next to the Role.

Security Dashboard User Guide

1	Server: LSF_PROD Product Line: LTMDEV				
2	Role	Security Class	Type	Object	Rule
476	DirectSupervisor_ST	UserFolderAllAccess_ST	BusinessClass	UserFolderItem	is accessible for all actions unconditionally
1145	Employee_ST	UserFolderAllAccess_ST	BusinessClass	UserFolder	is accessible for all actions unconditionally
1428	AbsenceAdmin_ST	UserFolderAllAccess_ST	BusinessClass	UserFolderItem	is accessible for all actions unconditionally
1834	Admin_ST	UserFolderAllAccess_ST	BusinessClass	UserFolderItem	is accessible for all actions unconditionally
2113	IndirectSupervisor_ST	UserFolderAllAccess_ST	BusinessClass	UserFolderItem	is accessible for all actions unconditionally
3079	HRGeneralist_ST	UserFolderAllAccess_ST	BusinessClass	UserFolder	is accessible for all actions unconditionally
3947	HRGeneralistActorOrgUnit_ST	UserFolderAllAccess_ST	BusinessClass	UserFolder	is accessible for all actions unconditionally
4426	ProxyDirectSupervisor_ST	UserFolderAllAccess_ST	BusinessClass	UserFolderItem	is accessible for all actions unconditionally
4655	LearningAdministrator_ST	UserFolderAllAccess_ST	BusinessClass	UserFolderItem	is accessible for all actions unconditionally
5451	HRGeneralistLite_ST	UserFolderAllAccess_ST	BusinessClass	UserFolder	is accessible for all actions unconditionally
5714	OccupationalHealthAdmin_ST	UserFolderAllAccess_ST	BusinessClass	UserFolderItem	is accessible for all actions unconditionally
5843	HRGeneralistEmploymentContract_ST	UserFolderAllAccess_ST	BusinessClass	UserFolder	is accessible for all actions unconditionally
6001	PositionBudgetManager_ST	UserFolderAllAccess_ST	BusinessClass	UserFolderItem	is accessible for all actions unconditionally
6511	HRGeneralistEmp_ST	UserFolderAllAccess_ST	BusinessClass	UserFolder	is accessible for all actions unconditionally
6594	ProcessServerAllAccess_ST	ProcessServerAllAccess_ST	BusinessClass	BusinessSubject	is accessible for all actions unconditionally
6839	ProxyBonusObjective_ST	UserFolderAllAccess_ST	BusinessClass	UserFolderItem	is accessible for all actions unconditionally
6991	IndirectSupervisorLite_ST	UserFolderAllAccess_ST	BusinessClass	UserFolderItem	is accessible for all actions unconditionally
7304	HiringManager_ST	UserFolderAllAccess_ST	BusinessClass	UserFolderItem	is accessible for all actions unconditionally
7387	ProxyLimitedMgrWebAppAccess_ST	TATextSearchAccess_ST	BusinessClass	JobRequisitionSearch	is accessible for RebuildTextSearchFields unconditionally
8000	HRGeneralistActorOrgUnitLite_ST	UserFolderAllAccess_ST	BusinessClass	UserFolder	is accessible for all actions unconditionally
8251	ProxySalaryAwarding_ST	UserFolderAllAccess_ST	BusinessClass	UserFolderItem	is accessible for all actions unconditionally
8380	HRGeneralistActorOrgUnitEmploymentContract_ST	UserFolderAllAccess_ST	BusinessClass	UserFolder	is accessible for all actions unconditionally
8642	GoalLeader_ST	UserFolderAllAccess_ST	BusinessClass	UserFolder	is accessible for all actions unconditionally
8954	FacilitySafetyManager_ST	UserFolderAllAccess_ST	BusinessClass	UserFolder	is accessible for all actions unconditionally
9059	ProxyUserRole_ST	UserFolderAllAccess_ST	BusinessClass	UserFolderItem	is accessible for all actions unconditionally
9346	FacilityHealthManager_ST	UserFolderAllAccess_ST	BusinessClass	UserFolderItem	is accessible for all actions unconditionally

Drilling

The drill feature (only available with the advanced reporting version) allows you to move up or down the security tree to view settings for Actors, Roles or Security Classes. The following drill assignments are available.

- Drill from a Role down to see the assigned Security Classes
- Drill from a Role up to see the assigned Actors.
- Drill from a Security Classes down to see the assigned Objects.
- Drill from a Security Class up to see the assigned Roles.

To execute a drill, click on the linked object you would like to review. In the example below I clicked on the **ABMProcessing_ST** Security Class and was provided the option of viewing the Roles assigned to ABMProcessing_ST or the Objects that are assigned the ABMProcessing_ST.

Security Dashboard User Guide

Drag a column and drop it here to group by that column

Role	Security Class	Type	Object	Rule
AbsenceAdmin_ST	GHRSetupInquiryAcce...	BusinessClass	PaymentSchedule	is accessible for all inquiries unconditionally
AbsenceAdmin_ST	ABMImportExport_ST	BusinessClass	EmployeeBalanceExport	is accessible for all actions unconditionally
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	LeaveOfAbsence	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	TemporaryGeneralLedgerPosting	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	EmployeeTransactionSummary	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	TimeOffRequest	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	TemporaryEmployeeAbsencePlanDates	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	EmployeeAbsenceTransaction	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	EmployeeAbsenceHoursAllocation	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	EmployeeLengthOfServiceHours	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	TemporaryEmployeeAbsencePlanUpdate	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	TemporaryEmployeeAbsencePlanCreate	is accessible for all actions when (Employee.IsNotEmployee) is access
AbsenceAdmin_ST	ABMProcessing_ST	BusinessClass	TemporaryEmployeeAbsencePlanTransfe...	is accessible for all actions when (Employee.IsNotEmployee) is access

By selecting **Role|Security Class** a new browser page will open displaying all of the Roles assigned to this Class.

Drag a column and drop it here to group by that column

Role	Security Class	Security Class DescriptY
HRGeneralist_ST	ABMProcessing_ST	
AbsenceAdmin_ST	ABMProcessing_ST	

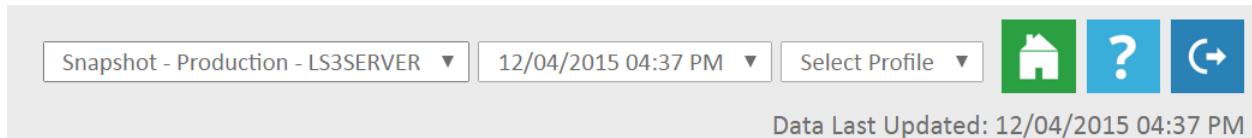
You can then drill on a specific Security Class to see the Business Classes and their associated rules.

Drag a column and drop it here to group by that column

Security Class	Security Class DescriptY	Type	Object	Rule
ABMProcessing_ST		BusinessClass	LeaveOfAbsence	is accessible for all actions when (Employee.IsNotEmployee) is accessible for all inq...
ABMProcessing_ST		BusinessClass	TemporaryGeneralLe...	is accessible for all actions when (Employee.IsNotEmployee) is accessible for all inq...
ABMProcessing_ST		BusinessClass	EmployeeTransactio...	is accessible for all actions when (Employee.IsNotEmployee) is accessible for all inq...
ABMProcessing_ST		BusinessClass	TimeOffRequest	is accessible for all actions when (Employee.IsNotEmployee) is accessible for all inq...
ABMProcessing_ST		BusinessClass	TemporaryEmployee...	is accessible for all actions when (Employee.IsNotEmployee) is accessible for all inq...
ABMProcessing_ST		BusinessClass	EmployeeAbsenceTr...	is accessible for all actions when (Employee.IsNotEmployee) is accessible for all inq...
ABMProcessing_ST		BusinessClass	EmployeeAbsenceH...	is accessible for all actions when (Employee.IsNotEmployee) is accessible for all inq...
ABMProcessing_ST		BusinessClass	EmployeeLengthOfS...	is accessible for all actions when (Employee.IsNotEmployee) is accessible for all inq...
ABMProcessing_ST		BusinessClass	TemporaryEmployee...	is accessible for all actions when (Employee.IsNotEmployee) is accessible for all inq...
ABMProcessing_ST		BusinessClass	TemporaryEmployee...	is accessible for all actions when (Employee.IsNotEmployee) is accessible for all inq...
ABMProcessing_ST		BusinessClass	TemporaryEmployee...	is accessible for all actions when (Employee.IsNotEmployee) is accessible for all inq...
ABMProcessing_ST		BusinessClass	TemporaryLeaveOfA...	is accessible for all actions when (Employee.IsNotEmployee) is accessible for all inq...
ABMProcessing_ST		BusinessClass	TemporaryEmployee...	is accessible for all actions when (Employee.IsNotEmployee) is accessible for all inq...
ABMProcessing_ST		BusinessClass	EmployeeHoursAlloc...	is accessible for all actions when (Employee.IsNotEmployee) is accessible for all inq...
ABMProcessing_ST		BusinessClass	EmployeeAbsencePl...	is accessible for all actions when (Employee.IsNotEmployee) is accessible for all inq...
ABMProcessing_ST		BusinessClass	EmployeeServiceRec...	is accessible for all actions when (Employee.IsNotEmployee) is accessible for all inq...
ABMProcessing_ST		BusinessClass	HROrganizationUnit	is accessible for EmployeeAbsencePlanCalculation, all inquiries when (HROrganiza...

Historical Reports

Historical Reports (only available with the advanced reporting version) support all of the functionality found in the standard reports. You can chose to run historical reports by selecting the appropriate "Snapshot" server, time stamp and profile in the top right corner of the screen.

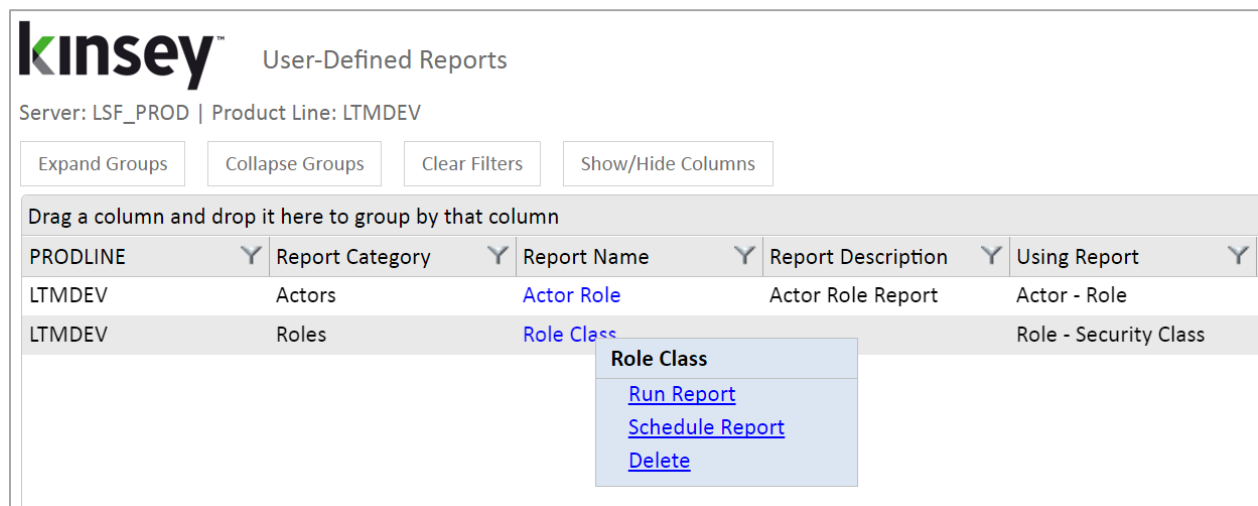


For more information on how to create Historical snapshots refer to the Kinsey Administrator Guide, page 12, Schedule Task.

Scheduling Security Reports

Scheduling (only available with the advanced reporting version) a report will allow you to automatically create and email any report you would like to receive on a regular basis.

To schedule a report you must first create and save your report. Once the report displays on the saved reports page you can click on the report name and select **Schedule Report**.



A grey clock icon is displayed at the end of the line if a schedule already exist for a report but has not been enabled. A blue clock icon indicates the the schedule is currently enabled.

Schedule Report

Select schedule to use: Select existing Create new schedule

Schedule name:

Every at :

Select users to email: Select existing Create new group

Email group name:

Email format:

Send blank reports:

The scheduling screen allows you to setup new schedules or use existing schedules. Schedules can be set to run each minute, hour, day, week, month or year.

You can also create or use existing report groups. A report group contains a list of users you want to receive the report.

Email format:

The export options are Excel or Adobe PDF

Send blank reports:

If you want the system to generate and send a report even if there is nothing to report select this option. This will inform the recipient that the report was run.

Deleting a Report

To delete a report, select the report name and click on Delete. You must have the proper permissions to delete a report.

Trouble Shooting

Why don't my security reports reflect my current changes?

If you are using the Advanced Landmark Reporting solution the security reports use data from SQL tables that are updated nightly. Any security changes made during the day will be reflected the following day. To see your changes immediately you need to run the scheduled task manually from the admin panel. For more information on how to run this task refer to the Kinsey Admin Users Guide, Scheduled Task.

If you are using the Free hosted version of Landmark Reporting the security reports use data uploaded to your system through our collection application. Any security changes made during the day will need to be uploaded to the reporting portal.

Notes: