TIBCO LogLogic® Compliance Manager User's Guide

Software Release 2.1.1
June 2017

Two-Second Advantage®

Important Information

Contents

Figures

TIBCO Documentation and Support Services

Documentation for this and other TIBCO products is available on the TIBCO Documentation site. This site is updated more frequently than any documentation that might be included with the product. To ensure that you are accessing the latest available help topics, visit:

https://docs.tibco.com

Product-Specific Documentation

The following documents for this product can be found on the TIBCO Documentation site:

- *Quick Start Guide*
- *User's Guide*
- *Release Notes*
- *Readme*

How to Contact TIBCO Support

For comments or problems with this manual or the software it addresses, contact TIBCO Support:

- For an overview of TIBCO Support, and information about getting started with TIBCO Support, visit this site:

  http://www.tibco.com/services/support

- If you already have a valid maintenance or support contract, visit this site:

  https://support.tibco.com

  Entry to this site requires a user name and password. If you do not have a user name, you can request one.

How to Join TIBCO Community

TIBCO Community is an online destination for TIBCO customers, partners, and resident experts. It is a place to share and access the collective experience of the TIBCO community. TIBCO Community offers forums, blogs, and access to a variety of resources. To register, go to the following web address:

https://community.tibco.com

Getting Started

Contents:

Logging in to LogLogic® Compliance Manager

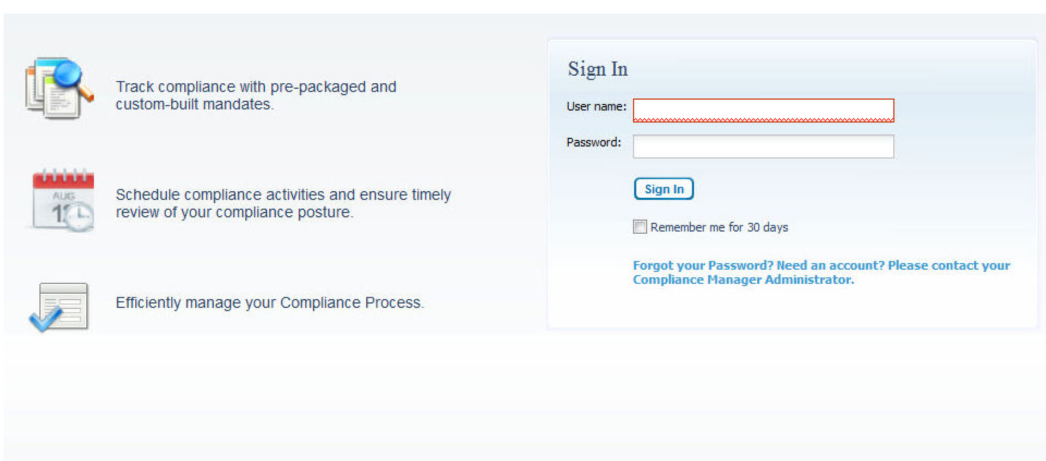
The following procedure explains how CM Users can log in to the application for the first time. If you are the CM Administrator, please see the procedure described in the 'Check the Connection of Your Web Browser' in the *TIBCO LogLogic® Compliance Manager Quick Start Guide*.

Whatever your role in CM, note that only one session can run properly on your workstation. If you open several sessions with different user accounts (either in the same web browser or on a different one), only the last opened user account is taken into account.

Procedure

1. Open a web browser on your workstation. See the list of supported web browsers in the *Quick Start Guide*.
2. Type the LogLogic® Compliance Manager Server URL (ask it to the CM administrator if you do not know it).

   CM Welcome Page



3. Log in by using the following default credentials:
   - User name: admin
   - Password: admin

   A **Change Password** dialog box opens, prompting you to change the default password
4. Enter a new password and click **Submit**. LogLogic® Compliance Manager opens.

User Roles

The LogLogic® Compliance Manager user interface is designed towards four primary user roles:

- Administrator Role
- Reviewer Role
- Executive Role
- Auditor Role

Administrator Role

The Administrator is responsible for installing and configuring the LogLogic® Compliance Manager. An administrator is someone who understands compliance requirements and is able to schedule reports to manage control objectives. The Administrator can:

- Enable the compliance review process by scheduling reports and specifying reviewers for the report results
- Manage exception handling processes for compliance activities
- Manage users' accounts and roles
- Review LogLogic® Compliance Manager application history
- Configure system wide settings for the LogLogic® Compliance Manager appliance
- Perform some or all Reviewer tasks depending on the company

In LogLogic® Compliance Manager, the primary work areas for Administrators are the **Review Management** and the **Administration** menus.

Reviewer Role

A user with this role performs detailed research and analysis. A Reviewer is required to periodically (daily or an alternate regular schedule) review log reports composed of user, system activity log data, and other application platforms and network activity data. They are also delegated the investigation tasks and are responsible for preparing summarized information for executives.

The Reviewer provides the critical human intelligence to identify and guide the organization compliance process.

In LogLogic® Compliance Manager, the work area for Reviewers is the Review Dashboard.

Executive Role

A user with this role has an at-a-glance view of the timeliness of the compliance activities and compliance ratings which includes the assessment by the compliance team. The Executives are the individuals who are ultimately accountable for the compliance initiatives and their success.

In LogLogic® Compliance Manager, the work area for Executives is the Executive Dashboard.

Auditor Role

A user who is given this role by the Administrator has an at-a-glance view of the Review process for the associated mandate.

The auditor both validates the compliance to mandates and checks that the LogLogic® Compliance Manager review process is correctly applied by the various CM users.

A distinction is made between the Internal Auditor Role and the External Auditor Role. The Internal Auditor's role is to prepare his/her organization to a compliance audit made by an External Auditor.

These two roles actually have the same abilities, except that the External Auditor cannot write comments. This functionality is indeed reserved to the Internal Auditor whether to point out specific things to the Reviewers or not.

The Auditor can therefore:

- Browse the review process summary for the associated mandate.
- Browse the review history and comment logs related to the associated mandate.
- Browse through the reports and drill-down through the report details.
- Send notifications to reviewers (Internal Auditors only).
- Insert auditor comments per mandate control (Internal Auditors only).

In LogLogic® Compliance Manager, the work area for Auditors is the Audit Dashboard.

First Time Administrator

An administrator typically performs the following tasks after initially installing the LogLogic® Compliance Manager solution:

Procedure

1. Add the Appliances that must be used by LogLogic® Compliance Manager in **Administration** > **Appliances**.
2. Add user accounts in **Administration** > **User Management**.
3. Enable the Mandates and Controls that must be enforced in your company in **Review Management** > **Mandate Management**.

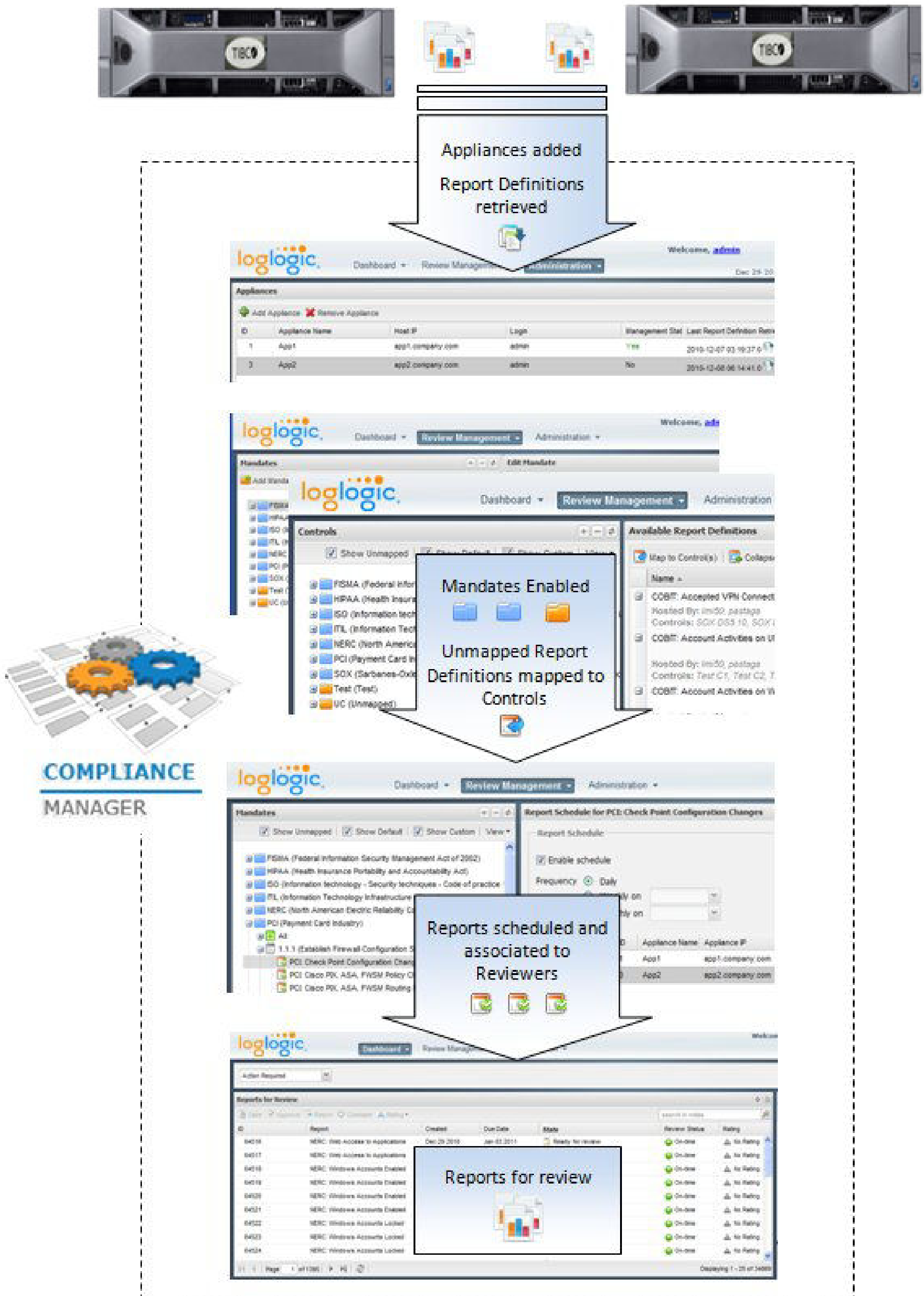
   You can add custom mandates and controls if your company has its own regulation requirements.
4. Associate Auditors and Executives to the various enabled mandates in **Administration** > **User Management**.
5. Map the unmapped report definitons retrieved from the Appliance(s) to Controls in **Review Management** > **Map Reports to Control**.
6. Schedule the reports that must be reviewed in **Review Management** > **Schedule Reports**.

   As an administrator, you will be able to control their reviews in **Review Management** > **Manage Reviews**.

   Users with Reviewer roles will be able to control their reviews in **Dashboard** > **Review** .

Report Process Configuration

The following graphic summarizes the overall report process configuration which is the fundamental task of the LogLogic® Compliance Manager administrator. Note that it focuses only on the forward progress of reports through CM, and therefore skips steps 2 and 4 described above which concerned the management of users.



First Time User

A user typically performs the following tasks when first getting access to the LogLogic® Compliance Manager:

- With a Reviewer role, the user reviews the reports in **Dashboard** > **Review**.
- With an Executive role, the user checks that the reports have been reviewed on time by Reviewers and that the overall compliance progress is OK in **Dashboard** > **Executive**.
- With an Auditor Role, the user checks that the review process has been followed as required in **Dashboard** > **Audit**.

Definition of Key Terms

Control

A control is a specific requirement that must be checked and verified, sometimes by external auditors. A mandate contains a large number of controls, there can be several hundreds of them. A Control includes a set of compliance reports (see “Report” definition).

Dashboard

A dashboard is a user interface that organizes and presents information in a way that is easy to read.

Mandate

A mandate can represent a government regulation (e.g., SOX), an industry regulation (e.g., PCI), a best practice framework (e.g., ISO) or a set of internal regulatory constraints enforced in the organization. It typically contains a list of requirements that an organization must satisfy. Mandates typically contain many controls (see “Control” definition).

Report

A report is activity log data (e.g., user escalations, firewall ports used, denied traffic, etc.) retrieved from a LogLogic appliance, and organized into an easy to understand format. It contains information which must be reviewed, approved, flagged, and/or escalated.

Report Definition

In LogLogic® Compliance Manager, a report definition is mapped to a mandate control by the administrator. Once the schedule and review management are defined for a report definition, instances of this report definition (i.e., reports) will be generated whenever information is retrieved from an appliance.

Report Result

Report results can be considered as summary views of similar report rows (referred to as report result details). They are displayed in all the views which contain a **Report** tab when a report is selected in a table.

Report Result Detail

A report result detail contains the list of messages detailing a specific report result. These messages are retrieved from a remote LMI appliance when the user clicks on the number displayed in the "Count" column of a report result (in the **Report** tab).

Report Schedule

A report schedule can be compared to a task generator. Each generated task contains a schedule phase and a review phase.

During the schedule phase, a report query is sent on one or several appliances to retrieve LMI report data at a precise time of the day*, depending on a query time range. The query time range can have a Daily, a Weekly or a Monthly frequency and always ends at midnight on the day that precedes the schedule phase. The aim of this schedule mechanism is therefore to retrieve report data on a continuous way even if its retrieval relies on segmented query time ranges.

* The task might not be executed at that very precise time of the day because all tasks are scheduled at the same time and they are processed one after the other.

Once the schedule phase is complete, the review phase begins. The report reviewers have to make a review of the report data retrieved during the schedule phase, respecting a due date.

Using Dashboards

A Dashboard is a user interface that organizes and presents information in a way that is easy to read. It can be compared to a canvas on which users with executive roles can add and move various types of modules showing the state of the system.

- Observation Periods in Dashboards
- Executive Dashboard
- Review Dashboard
- Audit Dashboard

Observation Periods in Dashboards

LogLogic® Compliance Manager can either use the default calendar year starting date (i.e. January 1st) or a custom year starting date if the **Financial Year Starting Date** property is customized in the **Administration** > **General Settings**menu.

The year starting date defined in this property will impact the Quarter to Date (QTD) and Year to Date (YTD) predefined observation periods that can be used in the CM Dashboards to monitor report data. Note that the Month to Date (MTD) predefined period is not impacted by this property definition.

For example, if the custom fiscal year starting date is set to March 13th and applied to YTD, this date will be used as the year starting date in all CM Dashboards. If it is applied to QTD, then Quarter 1 will begin on March 13th and the following Quarters will be shifted accordingly.

Executive Dashboard

The Executive dashboard provides an up-to-date view of the status of your organization's progress in meeting its mandate control objectives. It is accessible to users who have the Executive role, to view the timeliness of activity completion or the compliance rating at the Mandate and Control level in a variety of time frames as presented in the user interface.

- Description of the Executive Dashboard
- Monitoring Mandates
- Monitoring All Reports at Once
- Monitoring User Statistics
- Monitoring User Review
- Viewing Overdue Reports
- Printing Executive Reports
- Customizing the Executive Dashboard Layout

Description of the Executive Dashboard

The Executive Dashboard contains the following elements:

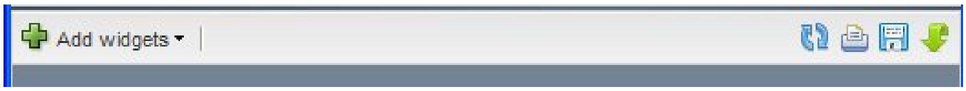
- Dashboard Toolbar
- Widgets

Please also see the following section: 'Tips About Columns in Widget Tables' for information about the use of columns in the various tables that can be found in several widgets.

Dashboard Toolbar

The toolbar at the top of the **Executive** dashboard displays several buttons which operate on the overall dashboard view.

Executive Dashboard Toolbar



Executive Dashboard: Toolbar Description

Button	Description
	Click this button to select the widgets you want to add to the dashboard. You can choose among the following widgets: • Mandates > <mandate name> • User Statistics • User Review • Overdue Reports • All Reports When you add widgets to the dashboard, the toolbar automatically refreshes to display their summary labels, e.g., PCI, FISMA, All Reports etc.  You can click/unclick these Summary labels to display/hide the widgets that have been added to the dashboard. For example, in the screenshot above, the PCI widget view is displayed on the dashboard and the All Reports widget is hidden.
	Click this button to refresh the dashboard view, that is to say the data shown in all the widgets currently present on the dashboard.
	Click this button to print the dashboard view. A Printable View Preferences dialog box opens to let you select the print parameters.
	Click this button to save the current layout of the dashboard view. All the widgets currently present on the dashboard as well their arrangement will be saved. This allows you to find the same arrangement whenever you open the Executive Dashboard.
	Click this button to restore the last saved layout after you have moved widgets on the dashboard.

Widgets

The following table lists the available widgets that can be added to the Executive dashboard and references to the sections that describe their use.

Executive Dashboard: Widget Descriptions

Widget	Description in...
Mandate	Monitoring Mandates
User Statistics	Monitoring User Statistics
User Review	Monitoring User Review
Overdue Reports	Viewing Overdue Reports
All Reports	Monitoring All Reports at Once

Tips About Columns in Widget Tables

- To sort a column by ascending or descending order, click once on its column header. Sorted columns have a dark grey header and their names are followed either by an upward (ascending) or a downward (descending) arrow.
- To rearrange the order/position of columns, drag-and-drop column headers on the column header row.
- To select the columns that you want to display, click the down triangle arrow on the right hand side of any column header, select the **Columns** menu and tick their corresponding check boxes.
- To resize columns to the desired width, mouseover their column dividers and click-and-drag the left/right arrow.

Monitoring Mandates

One of the Executive Dashboard functionalities consists in selecting and adding widgets corresponding to the available mandates to the workspace. It provides Executive users with a quick overview of the current review progress per compliance mandate (e.g. PCI, SOX, etc.).

Procedure

1. Select **Dashboard** > **Executive** from the navigation menu.
   The **Executive** view opens, displaying a toolbar and an empty workspace.
2. Click the Add widgets icon and select a mandate from the **Mandates** menu.

   A <**mandate name**> widget appears on the workspace displaying three tabs with information relative to the selected mandate.

   Mandate Widget Tabs

Mandate Widget: Tab Descriptions

<table>
<tr><th>Tab</th><th>Description</th></tr>
<tr><td>Summary</td><td>This tab displays a pie chart with the current review status, rating or state for the reports created in the chosen time interval. It therefore shows the relative proportion of reports which have:

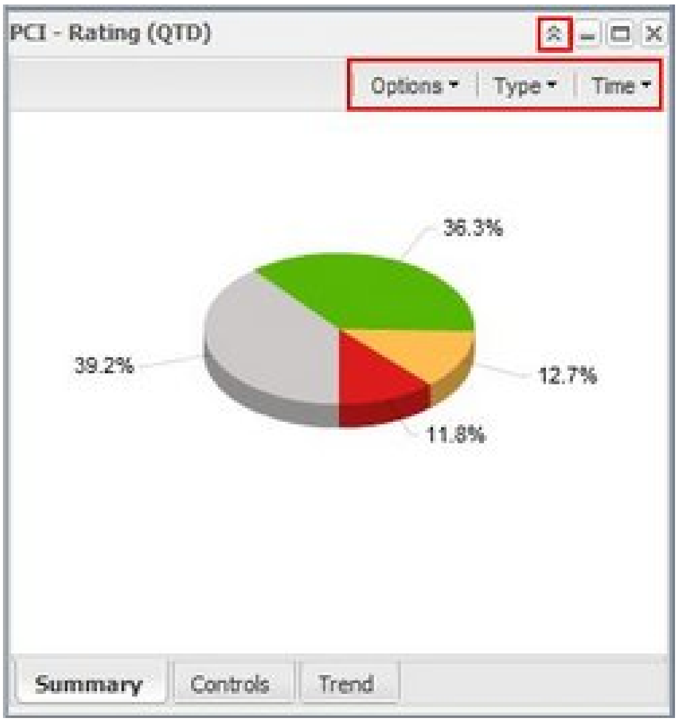
Review status:
On time
Approaching due date
Past due date
Rating:
No Rating
Low
Medium
High
State:
Ready for review
In review
Returned
Complete
This pie chart is interactive with the All Reports widget. You can therefore click one of its sectors to get filtered results in the All Reports widget.</td></tr>
</table>

Tab	Description
Controls	This tab displays a bar chart with the current review status, rating or state for the reports created in the chosen time interval, and distributed by mandate control. It therefore shows for each control the relative proportion of reports which have: **Review status**: • On time • Approaching due date • Past due date **Rating**: • No Rating • Low • Medium • High **State**: • Ready for review • In review • Returned • Complete This bar chart is interactive with the **All Reports** widget. You can therefore click one of its segments to get filtered results in the **All Reports** widget.
Trend	This tab displays a stacked bar chart with the daily Review Progresss over the chosen time interval. Each bar segment shows the number of reports for each review status: • On time • Approaching due date • Past due date This allows you to get an idea of the review evolution over time and point out the specific days when review activities went wrong.

Applying Filters and Options to the Mandate Widgets

Each Mandate widget contains a toolbar (available by clicking the double arrow icon), which allows you to filter the view. You just have to select a value in the pull-down menus displayed on the toolbar to get the view filtered accordingly.

Mandate Widget: Filters and Options



Filter/ Option	Description
Options	The pull-down menu contains the following filters: • **Include Reviewed Reports**: To include Reviewed Reports within the pie chart statistics • **Show Time Frame**: To display the time period selected above the pie chart. The time format used is MM/DD/YYYY, e.g., 10/22/2013 for October 22nd 2013. • **Show Chart Legend**: To display the pie chart legend.
Type (in the Summary and Controls tabs)	The **pull-down** menu allows you to select the type of statistics that you want to display that is, statistics on the **Review Status**, **Rating**, or **State**
Time	The **pull-down** menu allows you to filter on a period of time i.e., YTD, QTD, MTD, All, or Custom (by electing a start and an end date). The time format used is MM/DD/YYYY

Monitoring All Reports at Once

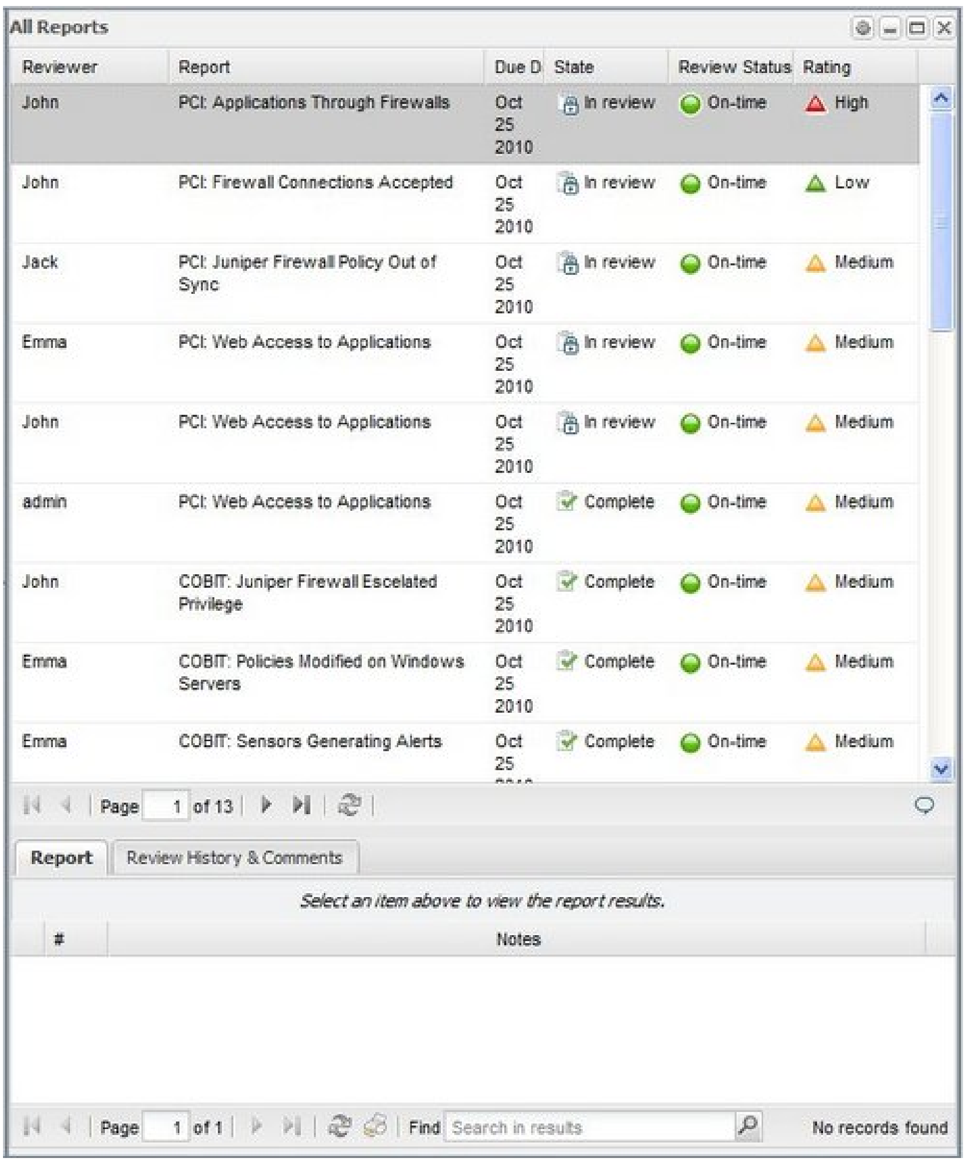
The Executive Dashboard gives you the possibility of having an overall view of all Report reviews at once, independantly from their respective mandates. This view shows the various reports currently under review with their Reviewers, due date, timeliness status, and rating.

Procedure

1. Select **Dashboard** > **Executive** from the navigation menu.
   The **Executive** view opens, displaying a toolbar and an empty workspace.
2. Click the Add widgets icon and select **All Reports** from the menu.

   An **All Reports** widget is displayed on the workspace displaying the current review progress of all reports for all reviewers along with the review due date, review state, review timeliness status, and reviewer-assigned rating.

   All reports widget



All Reports Widget Columns

Column	Description
ID	The numbered ID of the report
Control	The name of the control
Mandate	The name of the mandate
Reviewer	The name of the reviewer who is currently responsible of the report's review
Report	The name of the report
Due Date	The date the report must be completed by. See the description of the Review Status column, to learn how the due date is used to determine Compliance Review Timeliness
State	The current state of the report review: • Ready for Review: report has been retrieved from an appliance. • In Review: report has been claimed by a Reviewer. • Returned: a Final Reviewer has "returned" a report to a Reviewer for further analysis. • Complete: the Reviewers have approved the report.
Review Status	The review status indicates the current state of the report along with the state of the review process. • On time: The report review is on-time regarding the due date. • Approaching due date: The report review is very close to the due date. The default time allowed before a review is given a yellow status is 80% of the elapsed time between the Creation date and the Due date. This threshold can be changed in *General Settings*. • Past due date: The report review is over the due date.

Column	Description
Rating	This attribute of a report review activity is specified by the reviewer. The four states are: • No rating (no impact) • Low (minimal impact) • Medium (some impact) • High (High impact = High Risk) **Note:** The definition of Rating should be determined by your Compliance process and how you choose to interpret this value in Summary results.

Filtering and Sorting the Columns

The **All Reports** widget display can be filtered and/or sorted by any column displayed.

Procedure

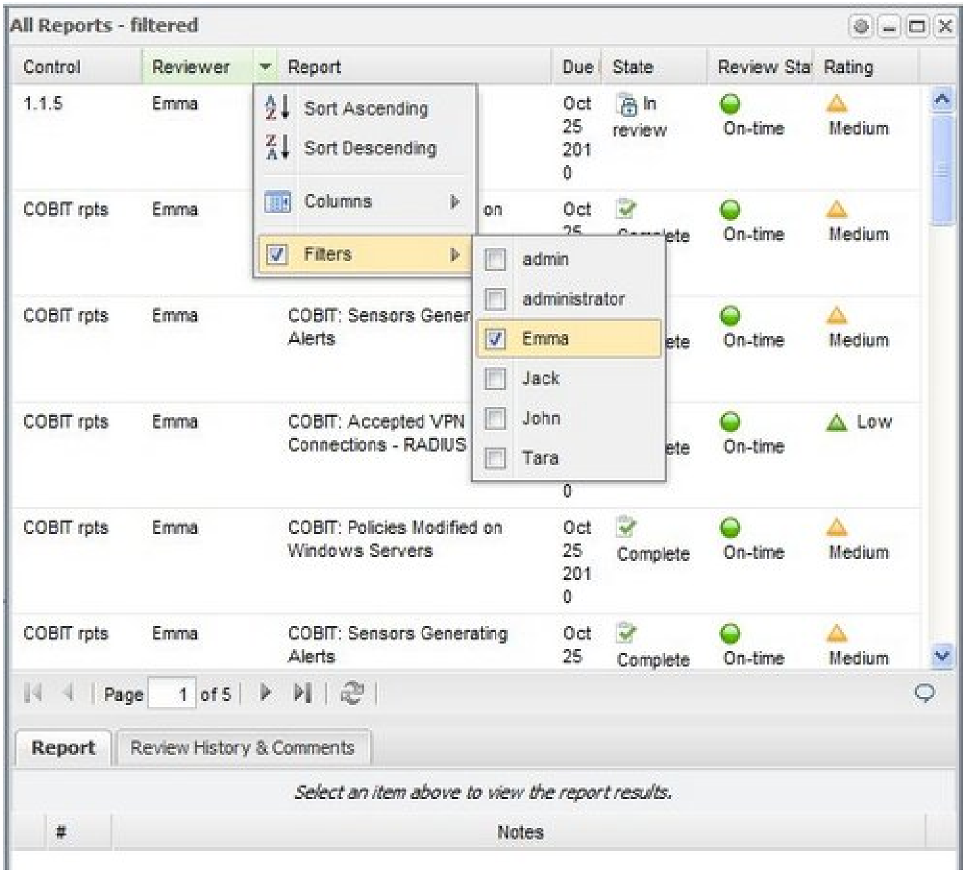
1. Click once on any column to change the sort order.

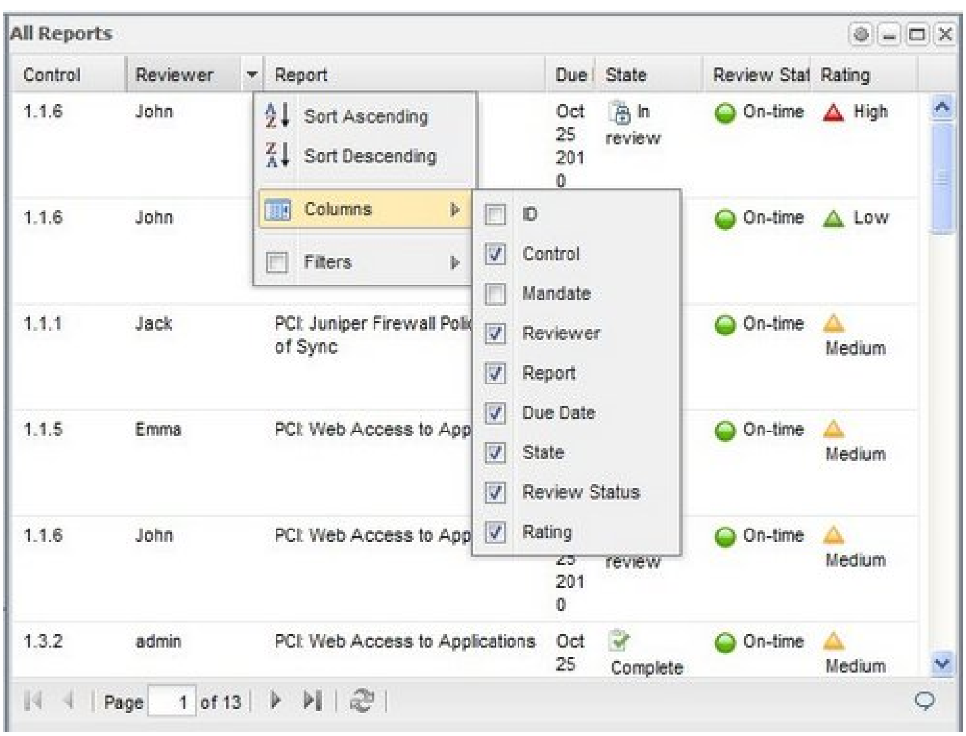
   To keep satisfying perfomances avoid sorting the columns: Control, Mandate, Report, Reviewer and Source Appliance.

2. To filter the view, mouseover the column header row and select the down triangle arrow to display the various applicable filters, i.e., **Sort Ascending, Sort Descending, Columns** (ID, Control, Mandate, Source Appliance, Reviewer, Report, Modified, Due Date, State, Review Status, Rating), and **Filters**.

   Examples:

   - To view Reviews corresponding to a single Reviewer, select the reviewer filter menu, then select the check box corresponding to the Reviewer’s user name.
   - To set the columns that should be displayed in the **All Reports** widget, select the Columns menu, then select the desired check boxes.





3. To clear all filter conditions, click the  button at the top of the widget.

Note: When you click another widget’s graphical view (example a pie chart or a bar chart segment), the **All Reports widget** view is filtered automatically to show only the corresponding data.

Adding a Comment to a Report

The Add Comment function allows the executive users to leave notes to the report reviewers.

Procedure

1. Select it in the All Reports list and click the **Add a comment to the report** button at the bottom right hand corner.
2. Type in a comment in the **Report Comment** dialog box and click the **Add comment** button. The comment is saved and added to the list of the **Review History & Comments** tab.

Monitoring Report Results

The **Report** tab contains a table displaying the results of the report selected above, in the **All Reports** panel. These report results can be considered as summary views of similar report rows. You can also see that many reports display a **Count** column to indicate precisely the number of rows corresponding to each report result. The count hyperlink allows you to drill-down to the report rows that is to the **Report Result Details** level.

On this tab, you can:

- Annotate report results. See Adding/Viewing Report Result Annotations for more details.
- Print report results. See Printing Report Results for more details.
- Drill-down to the report result details level (if a **Count** column is displayed in the tab). See Drilling-Down to the Report Result Details Level for more details.

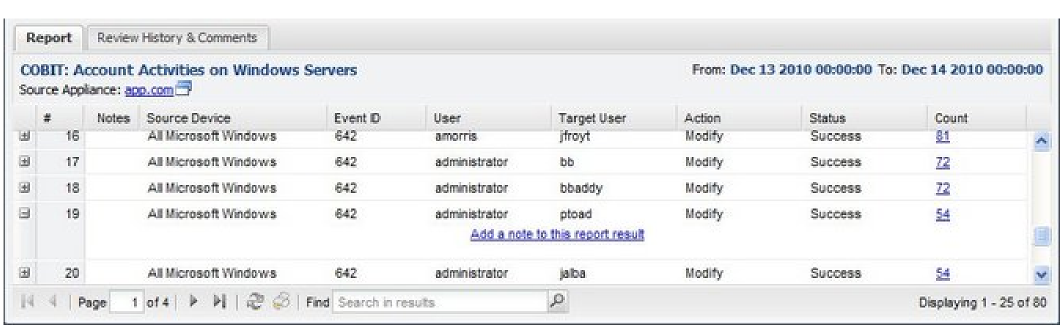
Adding/Viewing Report Result Annotations

Each result in a report can contain one or multiple annotations, or notes. You can do a fine-grain commenting of the report, down to the report result level. Report result annotations are archived and can be edited or deleted once created.

Procedure

1. Select a Report in the **Reports for Review** list.
2. Double-click a report result in the **Report** tab to expand it.

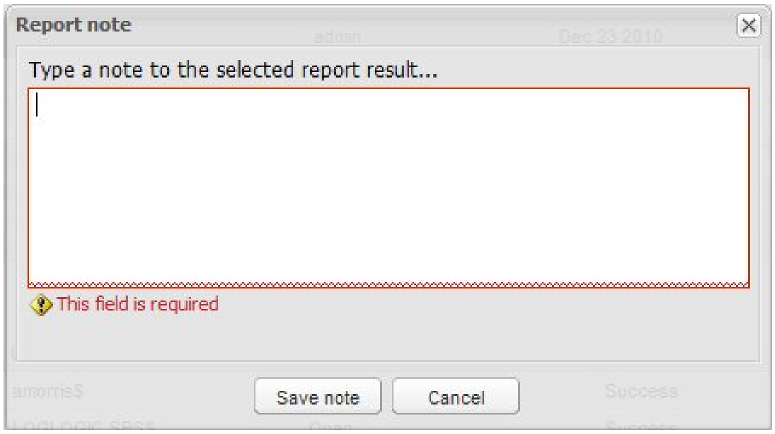
   Add a Note to this Report Result Link



3. Click the **Add a note to this report result** link.

   The **Report note** dialog box opens.

Report note Dialog Box

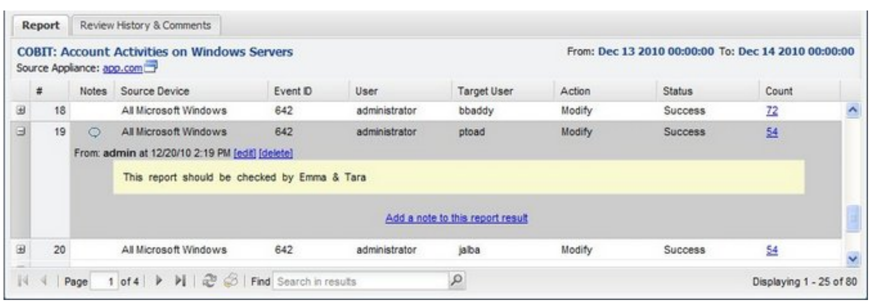


4. Type in your comment and click **Save note**.

   The Annotation is displayed below the report result with the timestamp of when the Annotation was created, and the User Account that created the Annotation.

   The report results that have an annotation, display an icon in the **Notes** column. Double-click the report result to display all its annotations.

Display of Report Result Annotation



The report result note can be edited or deleted by clicking the [Edit]/[Delete] links.

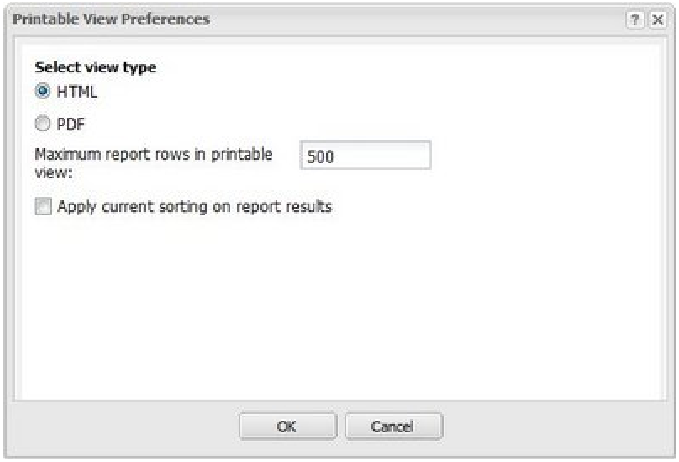
Printing Report Results

Procedure

1. Click the **printer** icon located at the bottom of **Report** tab.

   The **Printable View Preferences** window opens.

Report Results Printable View Preferences



2. In the **Printable View Preferences** window, set the Print settings as needed.

   Printable View Preferences

Setting	Description
HTML/PDF	Use these radio buttons to select the file format for the printable view, i.e., either **HTML** or **PDF**
Maximum report rows in printable view	Enter the maximum number of report rows that must be displayed in the printable view.
Apply current sorting on reports	Tick this check box if you want your report to reflect your sorting preferences.

3. Click **OK**.

   The report review is generated in the format you selected, i.e. HTML or PDF, suitable for sending to a printer or downloading for reviewing offline. The HTML and PDF versions contain the following information:

   - Report Name
   - Retrieval Time
   - Due Date
   - Name of the Current Reviewer
   - Source Appliance for the Report
   - Description of the report
   - List of controls the report addresses
   - List of Report History and Comment Events
   - Report Results including annotations

Drilling-Down to the Report Result Details Level

For the reports displaying a **Count** column, it is possible to drill-down to the **Report Result Details** level and see all the rows corresponding to each report result.

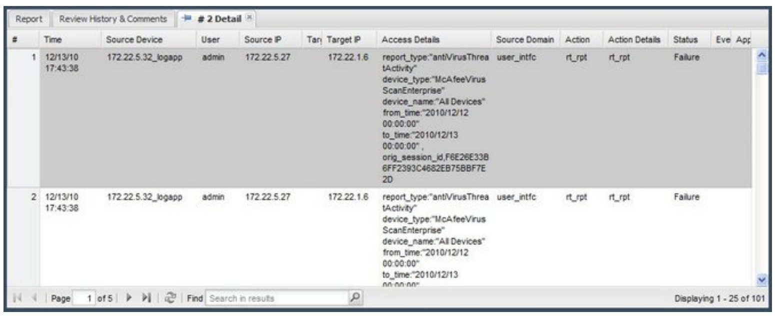
Drill-down actions depend on the appliance load and might therefore be very long (and sometimes fall in timeout). Obviously, the more powerful the hardware the faster the performances.

Procedure

1. In the **Count** column of the **Report** tab, click the hyperlink of a report result.

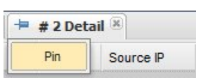
   A new tab appears in the bottom panel. Its label displays the line number of the report result (the format is # **<line number> Detail**) as shown in the **Report** tab. The generation of the report result details can take a few minutes.

   Report Result Details Tab



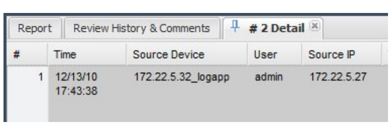
2. To save the report result detail tab for future use, mouseover the tab label and click **Pin** in the pop-up menu

   Report Result Detail Tab Pin Option



   Once pinned, the report result detail tab will always be displayed in the bottom panel of the Review dashboard when you select the same report in the **Reports for Review** panel

   Pinned Report Result Detail Tab



3. You can repeat the three first steps to open and pin more report result detail tabs.

   If you want to unpin a tab, mouseover its tab label and click **Unpin** in the the pop-up menu.

   All data of drill-down actions will be deleted from the CM database every 24 hours unless report result detail tabs are pinned.

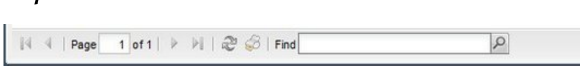
Searching in the Report tab

Use the **Find** box at the bottom of the panel to quickly filter the report results.

Procedure

1. Enter text into the **Find** box

   Report tab Find Box



2. Press **Enter**.

   The view will be filtered to display only the results containing the matching text (this text highlighted in bold characters).

Consulting the Review History & Comments

To view the change history and comment of a report review listed in the **Review Dashboard**, select it and consult the list displayed in the **Review History & Comments** tab.

Monitoring User Statistics

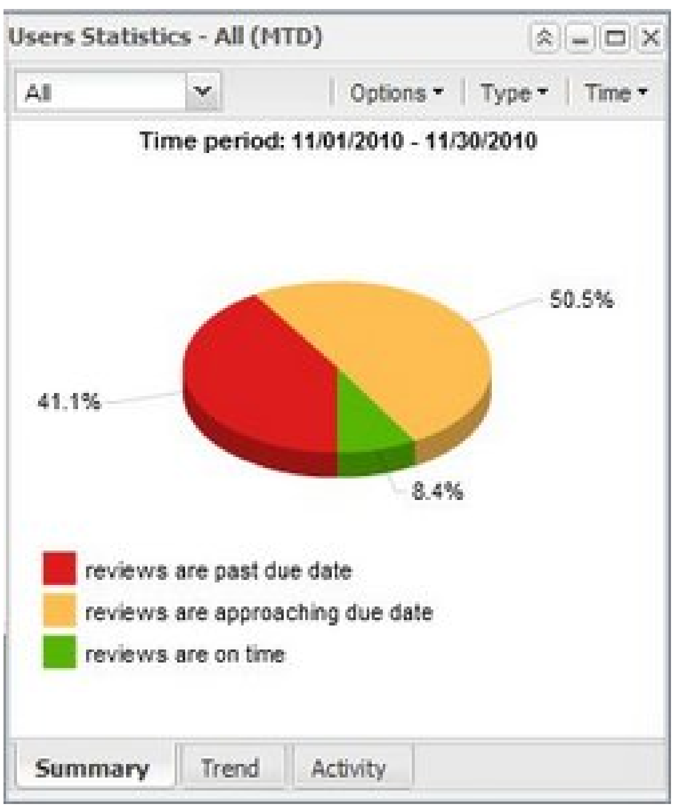
The **User Statistics** in **Executive Dashboard** monitors the progress status of the report reviews assigned to users.

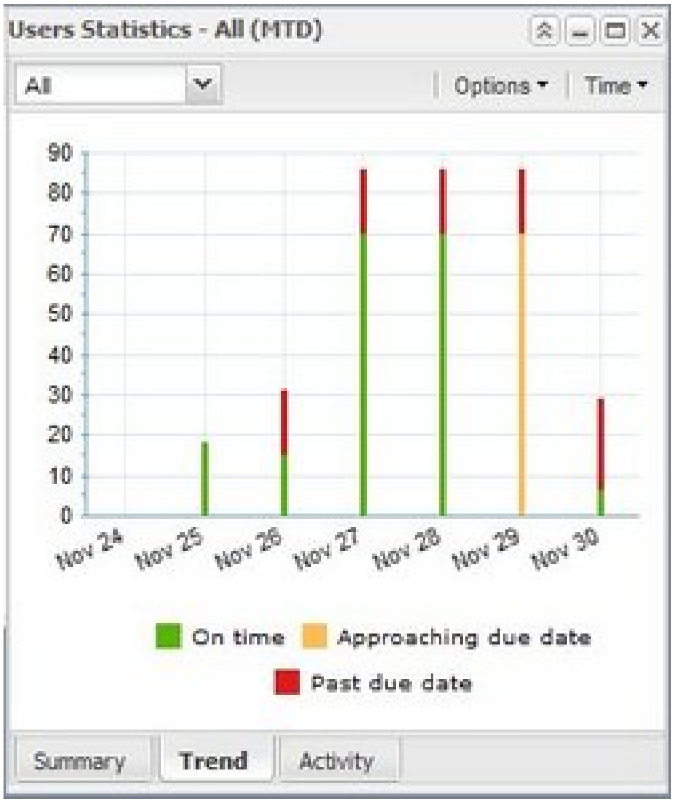
Procedure

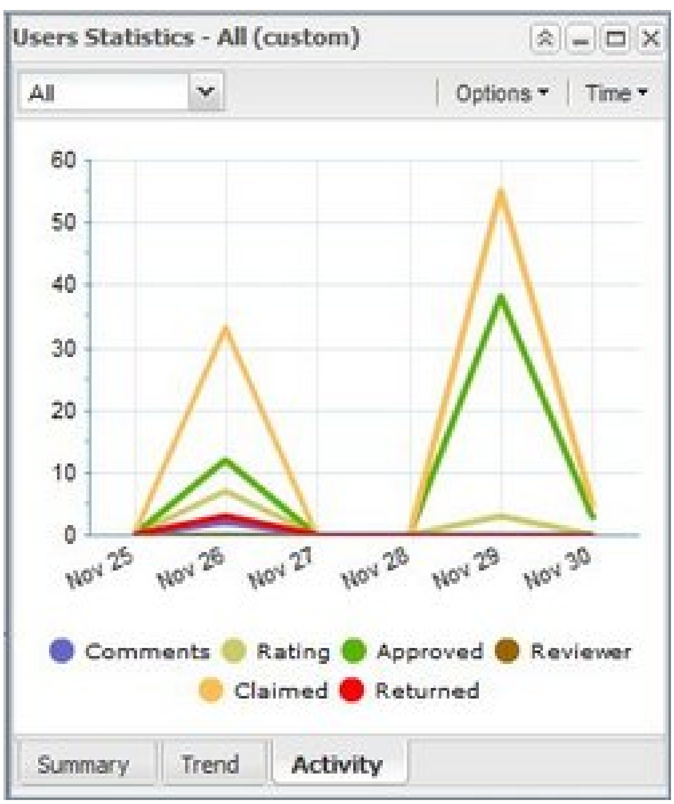
1. Select **Dashboard** > **Executive** from the navigation menu.
   The **Executive** view opens.
2. Click the **Add widgets** icon and select the **Users Statistics** menu item.

   A **Users Statistics** widget appears on the workspace displaying three tabs with information relative to the users' reviews

   User Statistics Widget Tabs


Users Statistics - All (MTD)
All
Options
Time
90
80
70
60
50
40
30
20
10
0
Nov 24
Nov 25
Nov 26
Nov 27
Nov 28
Nov 29
Nov 30
On time
Approaching due date
Past due date
Summary
Trend
Activity


Users Statistics - All (custom)
All
Options
Time
60
50
40
30
20
10
0
Nov 25
Nov 26
Nov 27
Nov 28
Nov 29
Nov 30
Comments
Rating
Approved
Reviewer
Claimed
Returned
Summary
Trend
Activity

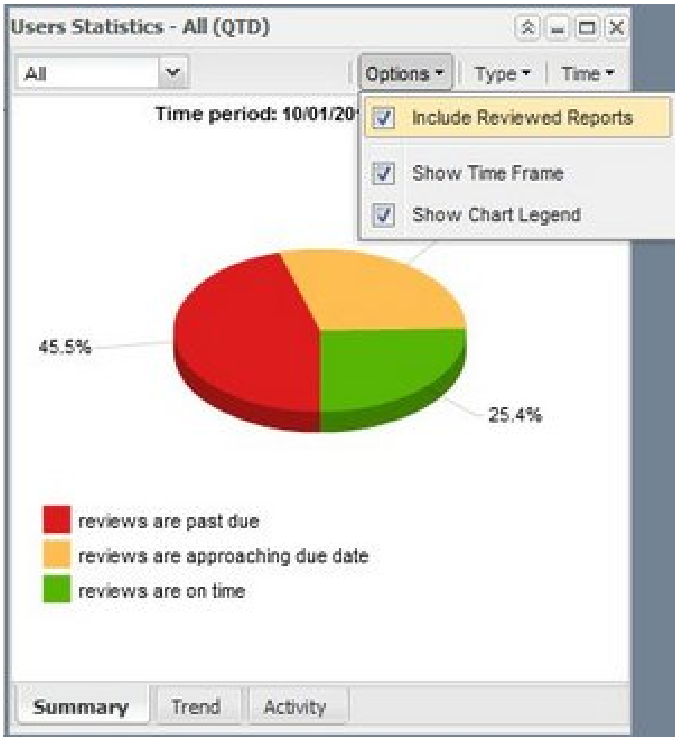
Mandate Widget: Tab Descriptions

Tab	Description
Summary	This tab displays a pie chart with the users' review progress in the chosen time interval. It gives an overview of the reviewers work showing the relative proportion of reports which have: **Review status**: • On time • Approaching due date • Past due date **Rating**: • No Rating • Low • Medium • High **State**: • Ready for review • In review • Returned • Complete This pie chart is interactive with the **All Reports** widget. You can therefore click one of its sectors to get filtered results in the **All Reports** widget.

Tab	Description
Trend	This tab displays a stacked bar chart with the users' daily Review Progress over the chosen time interval. Each bar segment shows the number of reports for each review status: • On time • Approaching due date • Past due date This allows you to get an idea of the review evolution over time and point out the specific days when review activities went wrong.
Activity	This tab displays a line chart with the users' activity peaks over the chosen time interval. It gives an idea of the progress of users' works over time for the following events: • Comment: Comment(s) added to the report history • Rating: Severity rating(s) changed for reports • Approved: Report(s) approved, i.e., set to Complete state and assigned to next reviewer (if any) • Reviewer: Reviewer(s) changed. This type of event occurs both when the first reviewer has completed a report and the latter is assigned to the final reviewer, and when the administrator reassigns a report to another reviewer. • Claimed: Reports claimed for review by reviewers • Returned: Reports returned to previous reviewers This allows you to get an idea of the review evolution over time and point out the specific days when review activities went wrong.

Applying Filters and Options to the User Statistics Widget

Each tab in the widget view contains a toolbar (available by clicking the double arrow icon) which allows you to filter the view. You just have to select a value in the pull-down menus displayed on the toolbar to get the view filtered accordingly



Toolbar Filters and Options

Filter/ Option	Description
All/<user names>	The pull-down menu allows you to filter on the users for whom you want to apply he statistics
Options	The pull-down menu contains the following filters: • **Include Reviewed Reports**: To include Reviewed Reports within the pie chart statistics • **Show Time Frame**: To display the time period selected above the pie chart. The time format used is MM/DD/YYYY, e.g., 10/22/2010 for October 22nd 2010. • **Show Chart Legend**: To display the pie chart legend.
Type (in the Summary tab only)	The pull-down menu allows you to select the type of statistics that you want to display i.e., statistics on the Review Status, Rating, or State
Time	The pull-down menu allows you to filter on a period of time i.e., YTD, QTD, MTD, All, or Custom (by selecting a start and an end date). The time format used is MM/DD/YYYY.

Monitoring User Review

User Review Widget Description

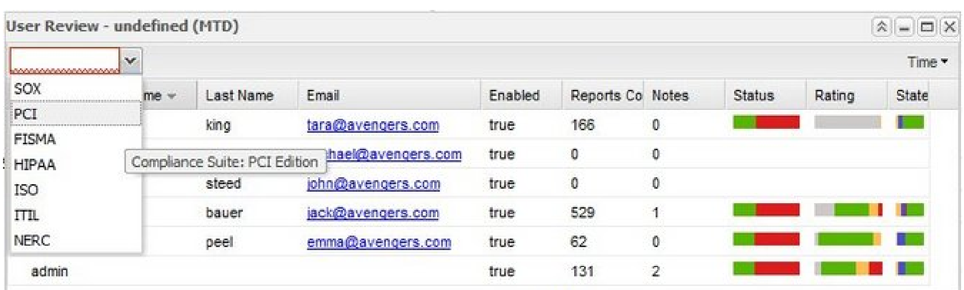
Column	Description
Login	Indicates the user's login
First Name	Indicates the user's first name
Last Name	Indicates the user's last name
Email	Indicates the user's email address
Enabled	Indicates whether the user account is currently enabled or disabled in CM
Reports Count	Indicates the number of reports retrieved assigned to the user
Notes	Indicates the number of reports which have been annotated.
Status	This column displays a bar chart with the report review statuses in the chosen time interval. It gives an overview of the reviewers work showing the relative proportion of reports which are: • On time • Approaching due date • Past due date **Note:** This bar chart is interactive with the **All Reports** widget. You can therefore click one of its segments to get filtered results in the **All Reports** widget.
Rating	This column displays a bar chart with the review ratings in the chosen time interval. It gives an overview of the relative proportion of reports which have the rating: • No Rating • Low • Medium • High **Note:** This bar chart is interactive with the **All Reports** widget. You can therefore click one of its segments to get filtered results in the **All Reports** widget.

Column	Description
State	This column displays a bar chart with the states of reports in the chosen time interval. It gives an overview of the relative proportion of reports which are: • Ready for review • In review • Returned • Complete **Note:** This bar chart is interactive with the **All Reports** widget. You can therefore click one of its segments to get filtered results in the **All Reports** widget.

Applying Filters and Options to the User Review Widget

The widget contains a toolbar (available by clicking the double arrow icon) which allows you to filter the view. You just have to select a value in the pull-down menus displayed on the toolbar to get the view filtered accordingly

User Review Filters



Toolbar Filters and Options

Filter/ Option	Description
Select Mandate	The pull-down menu allows you to filter the view by mandate.
Time	The pull-down menu allows you to filter on a period of time i.e., YTD, QTD, MTD, All, or Custom (by selecting a start and an end date). The time format used is MM/DD/YYYY.

Viewing Overdue Reports

The **Overdue Reports** widget shows the ovedue report reviews distribution by user. You can see who are the reviewers with the highest number of late report reviews. It therefore gives you an idea whether specific reviewers are always late.

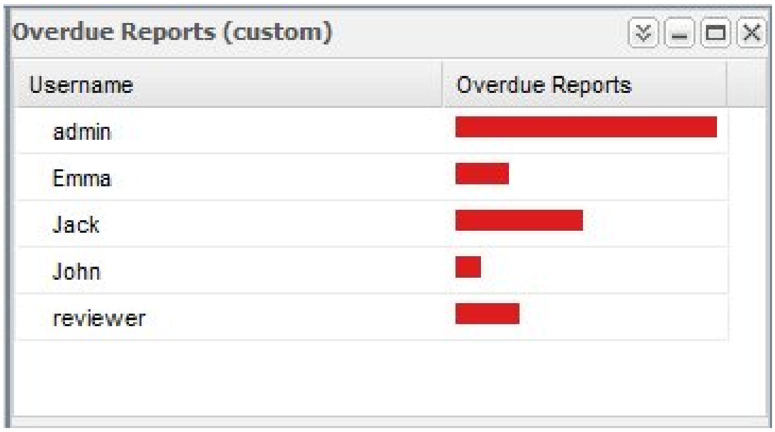
Procedure

1. Select **Dashboard** > **Executive** from the navigation menu.
   The **Executive** view opens.

2. Click the **Add widgets** icon and select the **Overdue Reports** menu item.

   An **Overdue Reports** widget appears on the workspace displaying a visual representation of the tasks which are past due date per user

   Overdue Reports Widget



3. Move the mouse pointer over the red bars to see the number of overdue reports for each user.

   Clicking the red bars allows you to filter the view in the **All Reports** widget interactively.

Applying Filters and Options to the Overdue Reports Widget

The widget contains a toolbar (available by clicking the double arrow icon) which allows to filter the view. You just have to select a value in the pull-down menus displayed on the toolbar to get the view filtered accordingly.

Toolbar Filters and Options

Filter/ Option	Description
Options	The pull-down menu contains a filter which allows to include Reviewed Reports within the statistics.
Time	The pull-down menu allows to filter on a period of time i.e., YTD, QTD, MTD, All

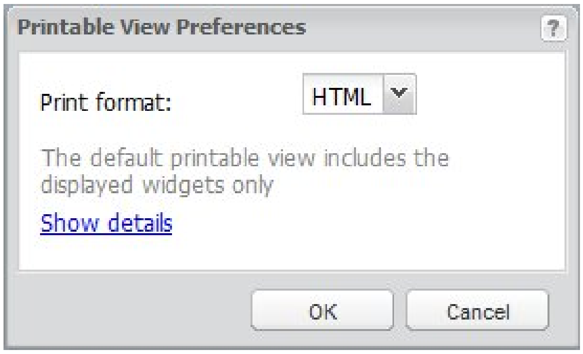
Printing Executive Reports

Procedure

1. Click the **print** icon on the button bar of the Executive dashboard.

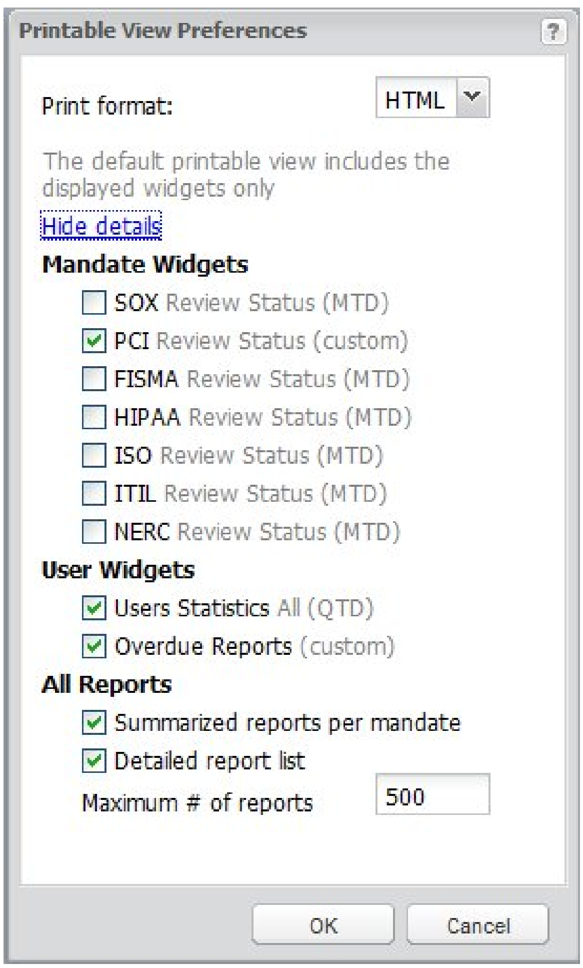
   The **Printable View Preferences** window opens

Executive Dashboard: Printable View Preferences



2. The default printable view includes only the widgets currently displayed on the dashboard. Click the Show details link if you want to see and refine the print settings details

Executive Dashboard: Printable View Preferences Displaying Details



3. Set the Print settings as needed.

Printable View Preferences

Setting	Description
Print format	Use the pull-down menu to select the file format for the printable view, i.e., either **HTML** or **PDF**

Setting	Description
Mandate Widgets	Tick the check box to include the mandated widgets to the printable view.
User Widgets	Tick the check boxes to include the user widgets to the printable view: • User Statistics • Overdue Reports,
All Reports	
Detailed report list	Tick this check box to get a view of the compliance activity details by: • New Reports for Review, • Previously Retrieved Reports, • Returned Reports, • High Rating Reports, • Overdue Reports, • Reviews Approaching Due Dates
Summary reports per mandate	Tick this check box to get a compliance summary per mandate: • All Reviews Timeliness Summary, • All Reviews Rating Summary, • Summary of number of reports by Compliance Control, • Returned Reports Summary by Compliance Control, • High Compliance Rating Reports Summary by Compliance Control • New Reports for Review Summary by Compliance Control, • Overdue Review Summary by Compliance Control, • Reviews Approaching Due Date Summary
Maximum number of reports	Enter the maximum number of reports that must be displayed in the printable view.

4. Click **OK**.

   The Executive dashboard printable view is generated in the format you selected, i.e., HTML or PDF.

Customizing the Executive Dashboard Layout

The Executive Dashboard can be seen as a global canvas on which you can place one or several modules wherever you want to have them displayed, organize them and change their sizes to get the best layout. It is based on a smart grid design which makes it easy to handle and get your own display.

Once you have defined your preferred layout, you can save it in order to get the very same view each time you use the Executive Dashboard. It is of course possible to modify the saved layout afterwards and save it once again. You can also restore the last saved layout if the changes you have made do not befit your needs.

Example of Executive Dashboard Customized Layout

Saving a Layout

Procedure

1. Click the **Save layout** button on the button bar of the Executive dashboard.
   The layout is saved.
2. Open another menu of the LogLogic® Compliance Manager application and go back to the Executive dashboard.
   The Executive dashboard displays your saved layout.

Restoring a Layout

Procedure

- Click the **Restore Layout** button on the button bar of the Executive dashboard.
  The saved layout is restored.

Review Dashboard

The **Review** dashboard lets you view the status of your report review progress, new reports that have been created or the reviews that have been returned/reassigned by an administrator or another reviewer. It also allows you to change the review states of reports to update your review progress.

- Description of the Review Dashboard
- Reviewing a Report
- Filtering and Sorting Reports
- Printing the Reports for Review List
- Monitoring Report Results
- Consulting the Review History & Comments

Description of the Review Dashboard

The Review Dashboard contains the following elements:

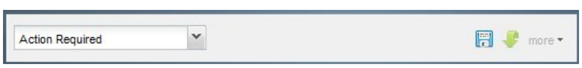
- Dashboard Toolbar
- Reports for Review Panel
- Compliance Progress Panel
- Control Objectives Panel
- Report Tab
- Review History and Comments Tab

Please also see the following section: Tips About Columns in the Review Dashboard Tables for information about the use of columns in the various tables that can be found in this view.

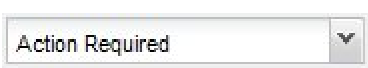
Dashboard Toolbar

The toolbar at the top of the **Review** dashboard displays several buttons which operate on the view displayed in the **Reports for Review** panel. You can define and save one or several filtered views and reuse them afterwards by selecting them from the toolbar pull-down menu. See Filtering and Sorting Reports for further information.

Review Dashboard Toolbar



Review Dashboard: Toolbar Description

Button	Description
	Click this pull-down menu to select the filtered view you want to apply to the dashboard. A filtered view is a set of filters applied to the **Report for Review** table. There are two predefined filtered views: • **No Filter**: Allows to get a view without any filters. It is therefore equivalent to the Clear all filter conditions button  . • **Action Required** (default filter): Allows to get a view of all reports requiring a user action, i.e., all reports except those which are in Complete state.
	Click this button to save the current filters applied to the dashboard view. This allows you to find and reuse filtered views whenever you open the Review Dashboard (by selecting them in the **Select Filter** pull-down menu). You can also choose to share a filtered view with all other reviewers.

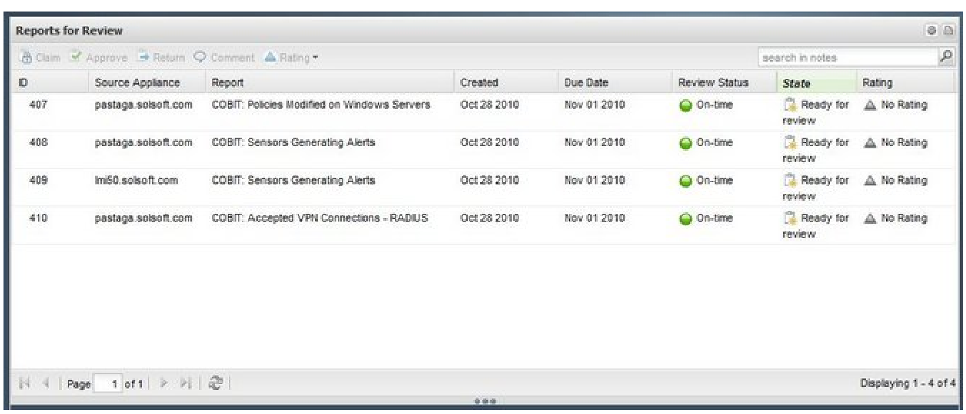
Button	Description
	Click this button to restore the last saved filters after you have made changes on the dashboard.
more	Click this pull-down menu to: • **Save as New**: Save the current filter with your modifications as a new filter. • **Delete**: Delete the current filter • **Share**: Enable/disable the saved filter sharing.

Reports for Review Panel

The **Reports for Review** panel lists all of the report results that must be reviewed to provide the needed evidence that the log collection and review activities were completed and make an assessment about the compliance posture of the organization

When a report is selected, the report results are displayed in the Report Tab, at the bottom of the screen. The Control Objectives Panel, located on the right, lists one or more control objectives that might be met by completing the review of the assigned report.

Reports for Review Panel



Reports for Review Panel Columns

Column	Description
ID	The numbered ID of the report results
Report	The name of the report
Created	The date the report results were queried and retrieved from the LogLogic Appliance
Due Date	The date the report must be completed by; see Review Status to learn how the due date is used to determine Compliance Review Timeliness

Column	Description
State	The current state of the report review: • Ready for Review • In Review • Returned • Complete
Review Status	The review status signifies the current state of the report along with the state of the review process. • On time: The report review is on-time regarding the due date. • Approaching due date: The report review is very close to the due date. The default time allowed before a review is given a yellow status is 80% of the elapsed time between the Creation date and the Due date. This threshold can be changed in *General Settings*. • Past due date: The report review is over the due date.
Rating	This attribute of a report review activity is specified by the reviewer. The four states are: • No rating (no impact) • Low (minimal impact) • Medium (some impact) • High (High impact = High Risk) **Note:** The definition of Rating should be determined by your Compliance process and how you choose to interpret this value in Summary results.

By default, some columns are hidden to show more important information. To view the hidden columns, click the down-arrow in a column heading and select the additional columns you want to view.

Reports for Review Buttons

Icon	Description
	Clears all filter conditions currently applied to the **Reports for Review** table.

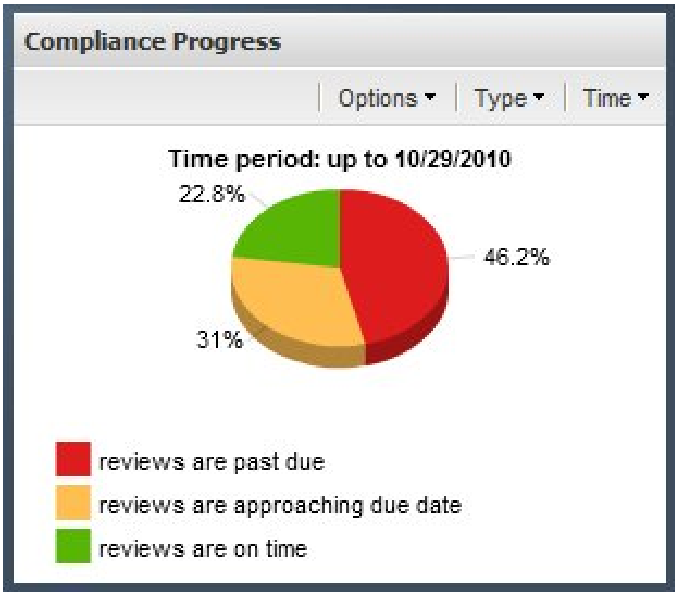
Icon	Description
	Opens the **Printable View Preferences** dialog box to let you select the format and the pages to include in the printable view of the Reports for Review table.
	Click this button to claim and review the selected report
	Click this button to approve the selected report The **Approve Report** text box appears. You can add a comment in the text box. Comments appear in the **Report History and Comments** for the report.
	Click this button to return the report to the previous reviewer **Note:** This applies only if you are the Final Reviewer of the report. The **Return Report to previous Reviewer** text box appears. You can add a comment in the text box. You can use this feature if you need more investigation to be completed by the prior reviewer. The comment you add at the report level is displayed in the **Report History and Comments** tab in the bottom frame.
	Click this button to add a comment to the selected report The **Report Comment** text box appears. The comment is a report level comment. Type your comment for the report then click **Add comment**. Comments appear in the **Report History and Comments** for the report.
	Click this button to select the severity rating for the selected report From the drop-down list, choose Low, Medium, or High. The default setting is "No Rating."
	Enter a text in the field and click the magnifying glass icon to launch the search in the Reports for Review table. Only the reports containing this text will be displayed in the table (the matching text will be displayed in **bold** characters).

Compliance Progress Panel

The **Compliance Progress** panel displays a pie chart, representing graphically the Review Status, Rating and State assigned to the reports. This pie chart is updated whenever a change is entered. The red color highlights the report reviews which have passed their due dates, the orange color highlights those which are approaching their due dates and the green color highlights the report reviews that were made on time.

Note that the time represented in the pie chart refers to the creation date of a report and not the due date. For example, if the only report in the system is created on January 30th and the due date is February 5th, the pie chart would display no data when the current time is February.

Compliance Progress Panel



The panel contains a toolbar (available by clicking the double arrow icon) which allows to filter the view. You just have to select a value in the pull-down menus displayed on the toolbar to get the view filtered accordingly.

Toolbar Filters and Options

Filter/ Option	Description
Options	The pull-down menu contains the following filters: • **Include Reviewed Reports**: To include Reviewed Reports within the pie chart statistics • **Show Time Frame**: To display the time period selected above the pie chart. The time format used is MM/DD/YYYY, e.g., 10/22/2010 for October 22nd 2010. • **Show Chart Legend**: To display the pie chart legend.
Type	The pull-down menu allows to select the type of statistics that you want to display i.e., statistics on the Review Status, Rating, or State
Time	The pull-down menu allows to filter on a period of time i.e., YTD, QTD, MTD, All, or Custom (by selecting a start and an end date). The time format used is MM/DD/YYYY.

Control Objectives Panel

If there are any controls associated with the selected report, you will see them in the **Control Objectives** panel. The controls for which the report is enabled are highlighted in bold characters.

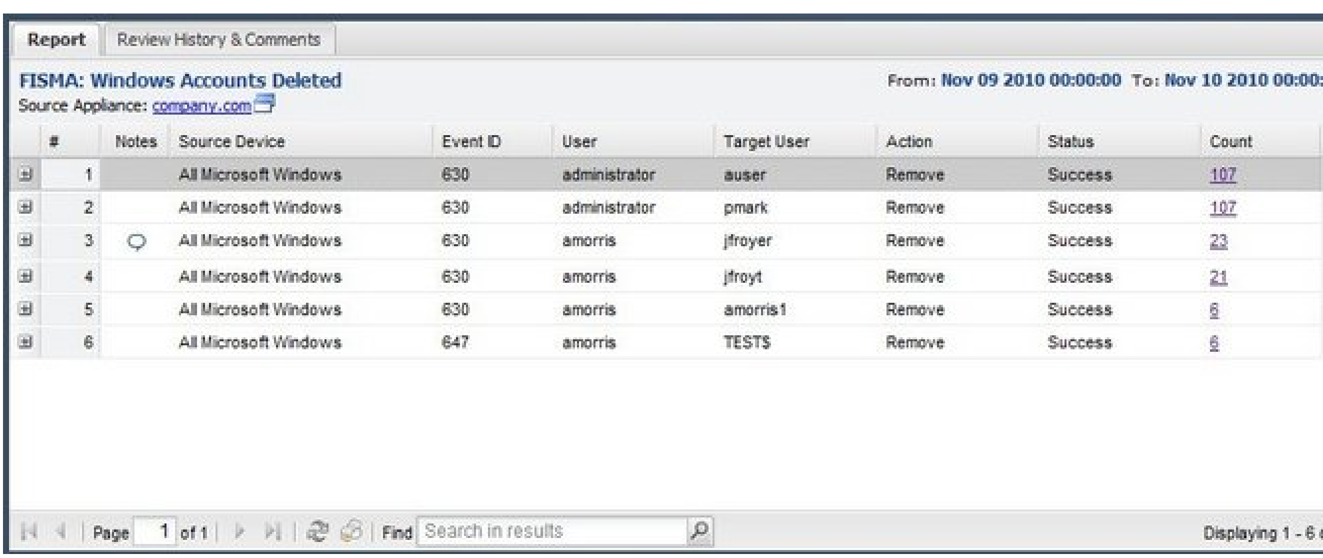
Control Objectives Panel

To view details about any Control, simply mouseover the Control Title.

Report Tab

The **Report** tab displays the Report Name, the query time range, the Appliance which the report was retrieved from, and the retrieval status of the report

Review Dashboard Report Tab



#	Notes	Source Device	Event ID	User	Target User	Action	Status	Count
1		All Microsoft Windows	630	administrator	auser	Remove	Success	107
2		All Microsoft Windows	630	administrator	pmark	Remove	Success	107
3		All Microsoft Windows	630	amorris	jfroyer	Remove	Success	23
4		All Microsoft Windows	630	amorris	jfroyt	Remove	Success	21
5		All Microsoft Windows	630	amorris	amorris1	Remove	Success	6
6		All Microsoft Windows	647	amorris	TESTS	Remove	Success	6

Report Tab Description

Item	Description
<Report Name>	The report name is displayed at the top left hand corner of the Report tab. It ispreceded by the name of the mandate it belongs to.
Report Query Time Range (From - To)	The Query Time range is time-relative to the appliance on which the report was retrieved. Report queries always use a query time range of midnight-to-midnight. This will include all report results for the day/week/month depending on the frequency selected.
Source Appliance	The **Source Appliance** link opens a new tab in your web browser window, allowing you to connect directly to the appliance where the report results were retrieved. This is provided to allow you to investigate any anomalies found in the Report Results.
Report Query Status	The Report Query Status, if any, is located below the Query Time Range. • If the Report query returned no results for the specified Query Time Range, then **No data available for specified report query** will be displayed. • If the report query exceeded the maximum result limit, then **Report result count exceeded max limit** will be displayed.
Column	**Description**
	The columns displayed in the **Report** tab depend on the report selected in the **Reports for Review** table. They therefore change dynamically depending on the selection made in that table.
#	The report result line number. A report result can be considered as a summary description of a group of report details (see Count definition below).
Notes	Report result annotations (if any) are flagged by a comment icon
Count	This column (displayed for many reports) indicates the number of details corresponding to the report result. Click the hyperlink to drill-down to the report result details level. See Drilling-Down to the Report Result Details Level.

Review History and Comments Tab

All events associated with a compliance report that is scheduled and assigned for review are recorded as documentation to meet the compliance activity documentation requirements of an audit. You can review the life cycle of a compliance report from the time of creation to completion in the **Review History & Comments** Tab

A list of events are recorded and time stamped when the report results were retrieved from the Appliance and the review entry was created, anytime the report state is changed by a Reviewer or Administrator (for example, when the report is Claimed, Returned, or Approved), or any comments added by a Reviewer or Administrator.

Review Dashboard Review History & Comments Tab


Report | Review History & Comments

ID	Date	Who	Event	Description
299	Dec 09 2010 14:58:30	admin	Comment	[Edit] [Delete] This report should be reviewed by Emma too.
223	Dec 08 2010 20:14:05	SYSTEM	Created	New report review entry 822 created for COBIT: Ports Denied Access - Nortel from MyApp2 for review by jack bauer.

Tips About Columns in the Review Dashboard Tables

- To sort a column by ascending or descending order, click once on its column header. Sorted columns have a dark grey header and their names are followed either by an upward (ascending) or a downward (descending) arrow.
- To rearrange the order/position of columns, drag-and-drop column headers on the column header row.
- To select the columns that you want to display, click the down triangle arrow on the right hand side of any column header, select the **Columns** menu and tick their corresponding check boxes.
- To resize columns to the desired width, mouseover their column dividers and click-and-drag the left/right arrow.

Reviewing a Report

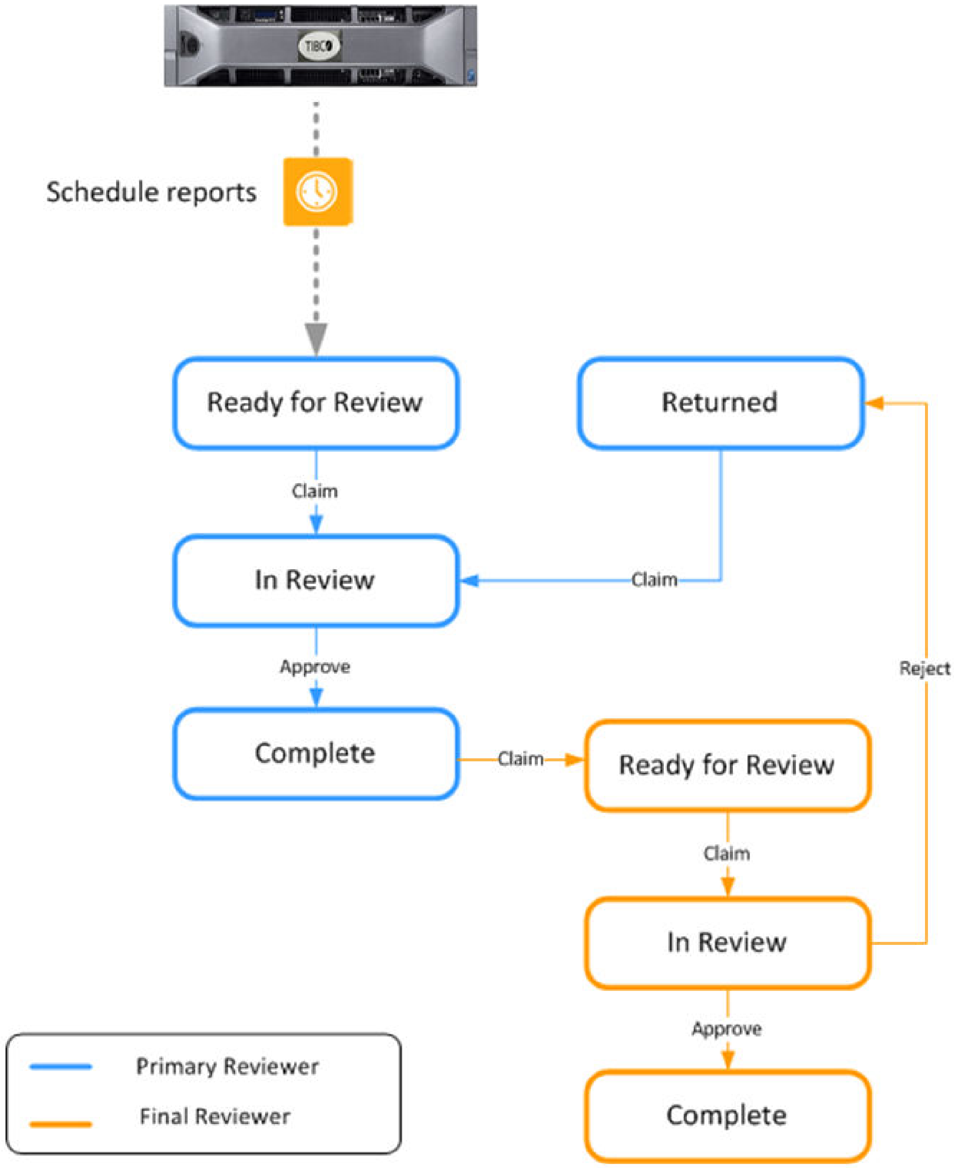
The report review process is based on a simple life cycle which is divided into the following steps:

Procedure

1. Primary reviewers receive in their dashboards scheduled reports retrieved from LogLogic appliances. These reports are in **Ready for review** state.
2. Primary reviewers claim the reports for review, that is to say that they mark these reports as being under analysis. These reports turn to **In Review** state.
3. Primary reviewers analyze the reports and approve them. These reports turn to **Complete** state.
4. Final reviewers (if any) receive the reports approved by primary reviewers. These reports are in **Ready for review** state. Final reviewers must then claim the reports (see step 2) and:
   - either approve the reports (reports turn to **Complete** state).
   - or reject and return reports to the primary reviewers (reports turn to **Returned** state).

   The review process life cycle can be summarized as in the following diagram.

Review Process Life Cycle



Contents

Claiming a Report for Review

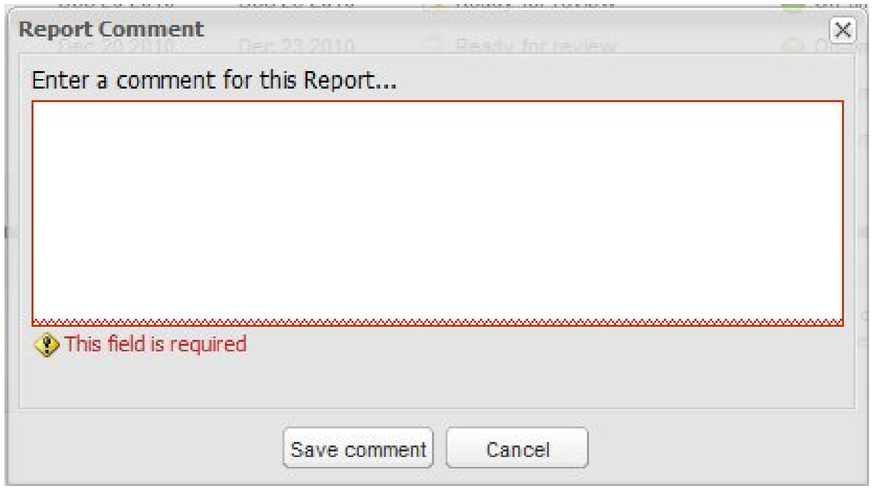
Procedure

1. Select a report in the **Reports for Review** panel.
   To select several reports at once, use the **Ctrl** and **SHIFT** keys.
2. Claim the report by clicking the **Claim** button.
   The state of the report will change from **Ready for Review** to **In Review**.
3. Optionally:

- Click the **Comment** button and type in your comment in the **Report Comment** dialog box if you want to annotate the report.

  The comment will be added to the table of the **Review History & Comments** panel.

Report Comment Dialog Box



- Click the **Rating** button to select the appropriate rating that must be assigned to the report.

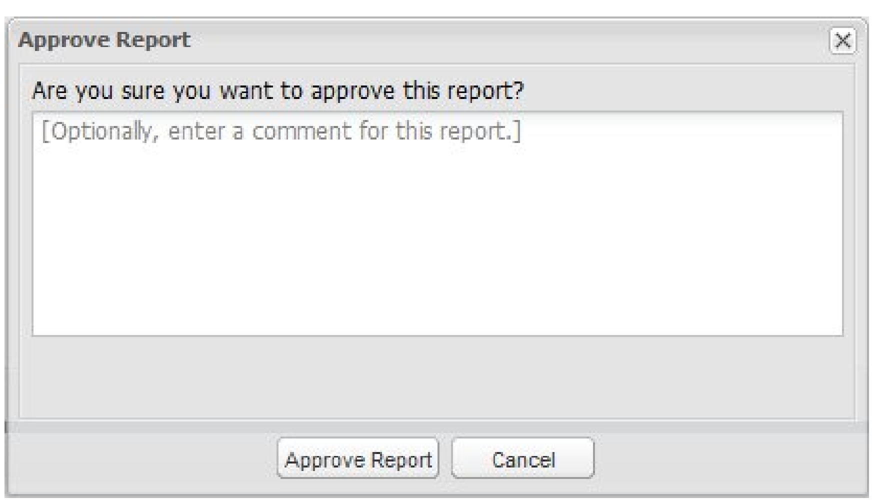
You can annotate or set the rating of several reports at once, by selecting them in the **Reports for Review** panel using the **Ctrl** and **SHIFT** keys and clicking the relevant buttons.

Approving a Report

Procedure

1. Select a report in the **Reports for Review** panel.
   To select several reports at once, use the **Ctrl** and **SHIFT** keys.
2. Approve the report by clicking the **Approve** button.
   The **Approve Report** dialog box opens

   Approve Report Dialog Box

3. Type in a comment if necessary and click the **Approve Report** button.

   The state of the report will change from **In Review** to Complete.

By default, if the task is completed, reports are not shown in the **Reports for Review** list. To include Completed reports in the list, mouseover the **State** column header, click the down triangle arrow and tick the **Filters** > **Complete** check box.

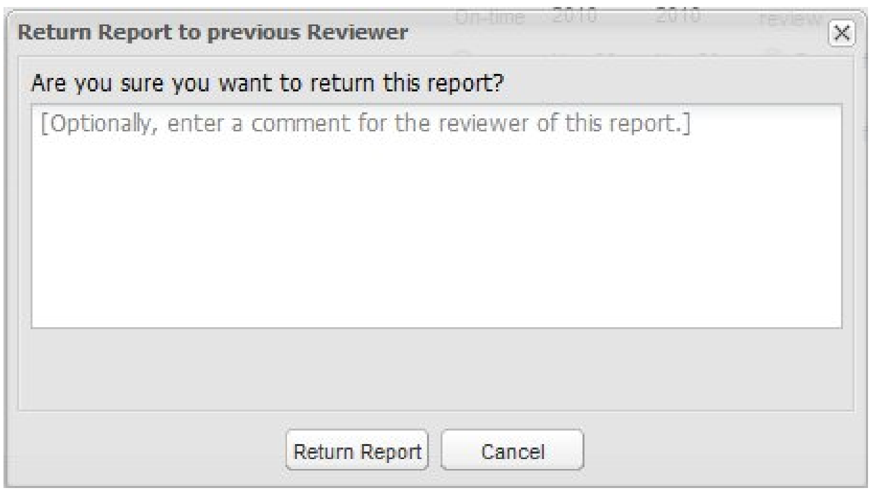
Returning a Report

Procedure

1. Select a report in the **Reports for Review** panel.
   To select several reports at once, use the **Ctrl** and **SHIFT** keys.
2. Return the report by clicking the **Return** button.

   The **Return Report to Previous Reviewer** dialog box opens

   Return Report to Previous Reviewer Dialog Box



3. Type in a comment if necessary and click the **Return Report** button.

   The state of the report will change from **In Review** to **Returned**.

   The report will be sent back to the primary reviewer who will see it as **Returned** in the **State** column of the **Reports for Review** panel, and have to follow the review process once again (i.e., claim and approve the report).

Filtering and Sorting Reports

The Reports for Review table display can be filtered and/or sorted by any column displayed. Filters can moreover be saved and shared to be reused by the CM Reviewers.

Contents

Applying Filters and Sorting to Reports

Procedure

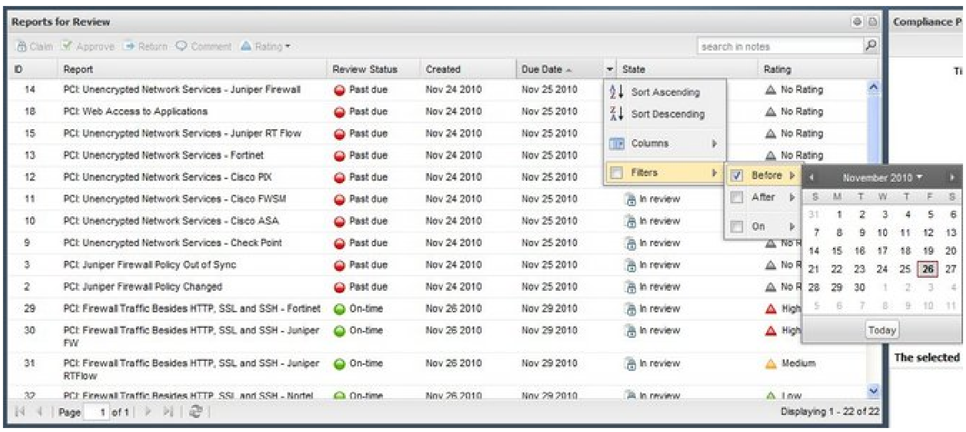
1. Click once on any column to change the sort order.

   To keep satisfying perfomances avoid sorting the columns: Report and Source Appliance.

2. To filter the view, mouseover the column header row and select the down triangle arrow to display the various applicable filters.

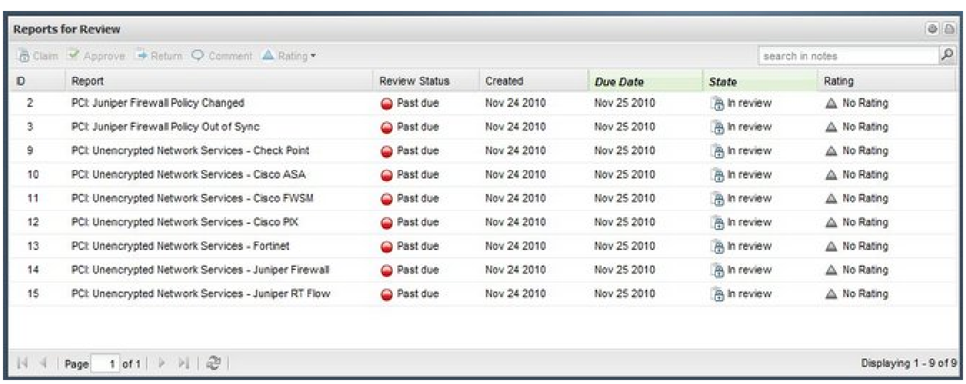
   For example, to filter on the Due Date, mouseover the **Due Date** column header, click the down triangle arrow, deploy the filters menu and select how (i.e., Before, After, On) and from which date the filter should be based on

   Report Filters for Due Date Column



   Columns on which filters have been applied can be easily located because their headers are highlighted both by a green background and a bold italic text.

   Filtered Columns Display



   You can also use the two predefined filters, i.e., No Filter or Action Required (default filter when you open the Review dashboard). No Filter removes all filter conditions and Action Required displays only the reports requiring a user action (i.e., all reports except those which are in Complete state).

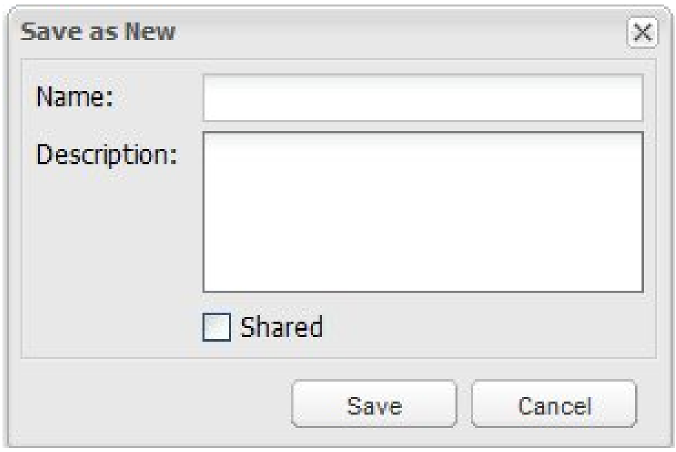
Saving Report Filters

Procedure

1. Click **Save Filter** to save the filtered view.

   The **Save as New** dialog box opens

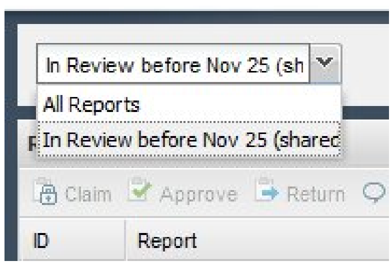
Save as New Dialog Box



2. Enter a name and a description, and tick the **Shared** check box if you want to share the filter with all other Reviewers.
3. Click **Save**.

   The filter is now added to the list of filters in the toolbar

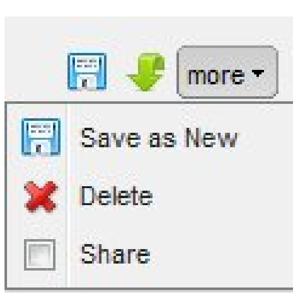
   Filter added to the List of Filters in the Toolbar



4. To edit/delete/or create a new filter from this filter, click the more pull-down menu in the toolbar and select the desired option

- **Save as New**: Save the current filter with your modifications as a new filter.
-  **Delete**: Delete the current filter
- **Share**: Enable/disable the saved filter sharing.

More Pull-down Menu Options in the Toolbar



Clearing Report Filter Conditions

Procedure

- To clear all filter conditions, click the  button at the top of the panel.

All filters will be removed from the **Reports for Review** table.

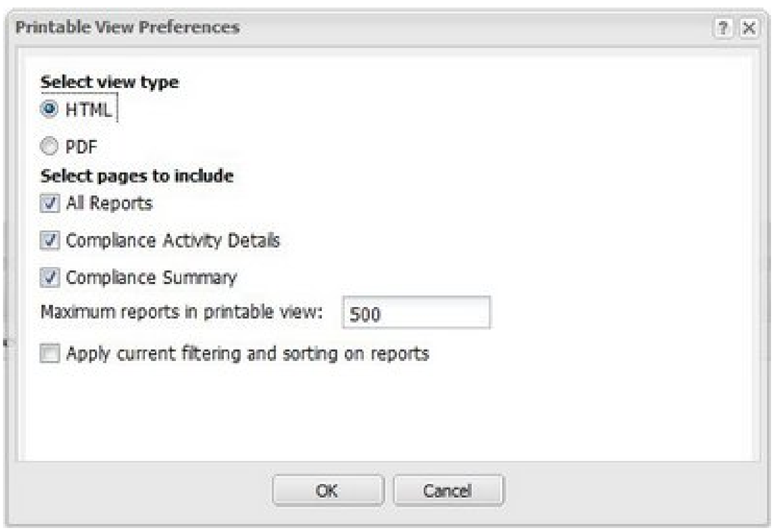
The removal of filter conditions does not apply to column sorting. The ascending/ descending order applied to a column will not be removed.

Printing the Reports for Review List

Procedure

1. Click the printer icon located in the **Reports for Review** title bar.
   The **Printable View Preferences** window opens

   Review Dashboard Printable View Preferences

2. In the **Printable View Preferences** window, set the Print settings as needed.

   Printable View Preferences

Setting	Description
HTML/PDF	Use these radio buttons to select the file format for the printable view, i.e., either **HTML** or **PDF**
All Reports	Tick this check box to print all reports.
Compliance Activity Details	Tick this check box to get a detailed breakdown of the report for review by: • New Reports for Review, • Previously Retrieved Reports, • Returned Reports, • Overdue Reports, • and Reviews are approaching due date

Setting	Description
Compliance Summary	Tick this check box to get a compliance summary covering: • All Reviews Timeliness Summary, • Summary of number of reports by Compliance Control, • Returned Reports Summary by Compliance Control, • New Reports for Review Summary by Compliance Control, • Overdue Review Summary by Compliance Control, • and Reviews Approaching Due Date Summary
Maximum # of reports	Enter the maximum number of reports that must be displayed in the printable view.
Apply current filtering and sorting on reports	Tick this check box if you want your report to reflect your filtering and sorting preferences.

3. Click **OK**.
   The report review is generated in the format you selected, i.e. HTML or PDF.

Monitoring Report Results

The **Report** tab contains a table displaying the results of the report selected above, in the **All Reports** panel. These report results can be considered as summary views of similar report rows. You can also see that many reports display a **Count** column to indicate precisely the number of rows corresponding to each report result. The count hyperlink allows you to drill-down to the report rows that is to the **Report Result Details** level.

On this tab, you can:

- Annotate report results. See Adding/Viewing Report Result Annotations for more details.
- Print report results. See Printing Report Results for more details.
- Drill-down to the report result details level (if a **Count** column is displayed in the tab). See Drilling-Down to the Report Result Details Level for more details.

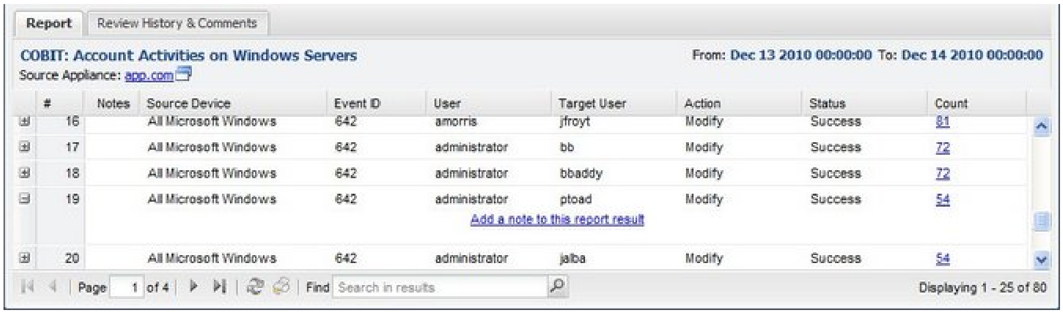
Adding/Viewing Report Result Annotations

Each result in a report can contain one or multiple annotations, or notes. You can do a fine-grain commenting of the report, down to the report result level. Report result annotations are archived and can be edited or deleted once created.

Procedure

1. Select a Report in the **Reports for Review** list.
2. Double-click a report result in the **Report** tab to expand it.

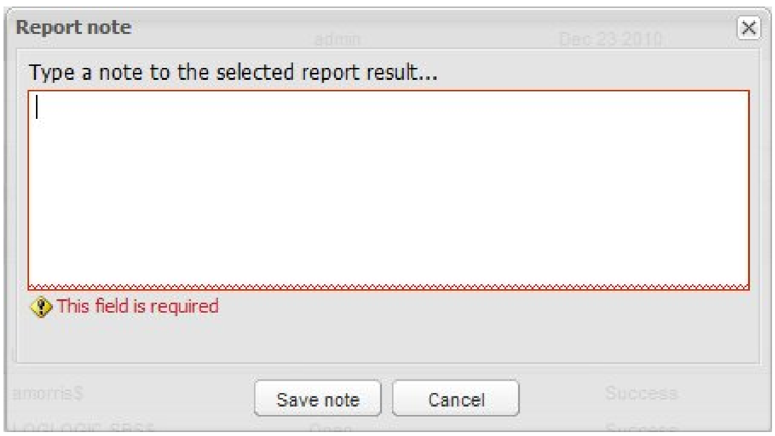
Add a Note to this Report Result Link



3. Click the **Add a note to this report result** link.

   The **Report note** dialog box opens.

   Report note Dialog Box

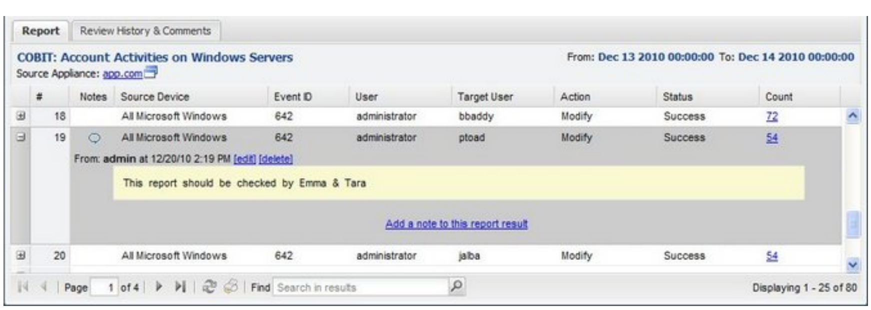


4. Type in your comment and click **Save note**.

   The Annotation is displayed below the report result with the timestamp of when the Annotation was created, and the User Account that created the Annotation.

   The report results that have an annotation, display an icon in the **Notes** column. Double-click the report result to display all its annotations.

   Display of Report Result Annotation



The report result note can be edited or deleted by clicking the [Edit]/[Delete] links.

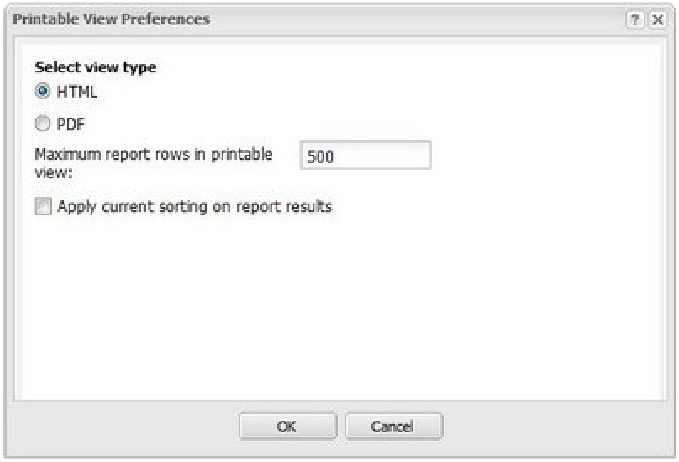
Printing Report Results

Procedure

1. Click the **printer** icon located at the bottom of **Report** tab.

   The **Printable View Preferences** window opens.

Report Results Printable View Preferences



2. In the **Printable View Preferences** window, set the Print settings as needed.

   Printable View Preferences

Setting	Description
HTML/PDF	Use these radio buttons to select the file format for the printable view, i.e., either **HTML** or **PDF**
Maximum report rows in printable view	Enter the maximum number of report rows that must be displayed in the printable view.
Apply current sorting on reports	Tick this check box if you want your report to reflect your sorting preferences.

3. Click **OK**.

   The report review is generated in the format you selected, i.e. HTML or PDF, suitable for sending to a printer or downloading for reviewing offline. The HTML and PDF versions contain the following information:

   - Report Name
   - Retrieval Time
   - Due Date
   - Name of the Current Reviewer
   - Source Appliance for the Report
   - Description of the report
   - List of controls the report addresses
   - List of Report History and Comment Events
   - Report Results including annotations

Drilling-Down to the Report Result Details Level

For the reports displaying a **Count** column, it is possible to drill-down to the **Report Result Details** level and see all the rows corresponding to each report result.

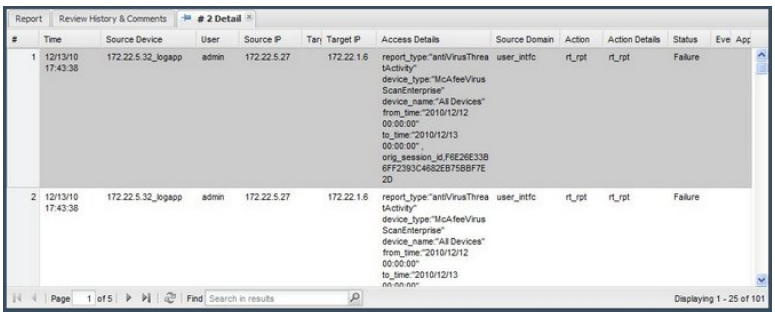
Drill-down actions depend on the appliance load and might therefore be very long (and sometimes fall in timeout). Obviously, the more powerful the hardware the faster the performances.

Procedure

1. In the **Count** column of the **Report** tab, click the hyperlink of a report result.

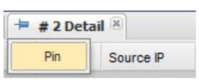
   A new tab appears in the bottom panel. Its label displays the line number of the report result (the format is # **<line number> Detail**) as shown in the **Report** tab. The generation of the report result details can take a few minutes.

   Report Result Details Tab

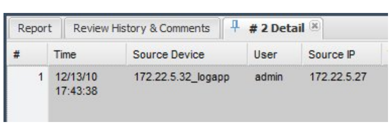
2. To save the report result detail tab for future use, mouseover the tab label and click **Pin** in the pop-up menu

   Report Result Detail Tab Pin Option

   Once pinned, the report result detail tab will always be displayed in the bottom panel of the Review dashboard when you select the same report in the **Reports for Review** panel

   Pinned Report Result Detail Tab

3. You can repeat the three first steps to open and pin more report result detail tabs.

   If you want to unpin a tab, mouseover its tab label and click **Unpin** in the the pop-up menu.

   All data of drill-down actions will be deleted from the CM database every 24 hours unless report result detail tabs are pinned.

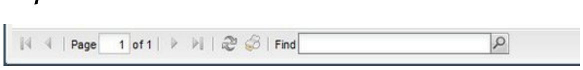
Searching in the Report tab

Use the **Find** box at the bottom of the panel to quickly filter the report results.

Procedure

1. Enter text into the **Find** box

   Report tab Find Box

2. Press **Enter**.

   The view will be filtered to display only the results containing the matching text (this text highlighted in bold characters).

Consulting the Review History & Comments

To view the change history and comment of a report review listed in the **Review Dashboard**, select it and consult the list displayed in the **Review History & Comments** tab.

Audit Dashboard

The **Audit** dashboard allows to get a quick view, or one could say, the evidence that compliance reports have been properly cycled into a formal review process. It is accessible to users who have the External or Internal Auditor role, to assess the review status per mandate over a defined period.

Contents

Description of the Audit Dashboard

The **Audit** Dashboard contains the following elements:

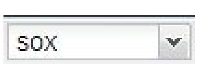
- Pull-Down Menu
- Left Panel
- Control Tab
- Review History and Comments Tab

Please also see the following section: Tips About Columns in the Audit Dashboard Tables for information about the use of columns in the various tables that can be found in this view.

Pull Down Menu

The pull-down menu at the top of the Audit dashboard allows to select the mandate on which the Audit must be performed

Audit Dashboard Pull-Down Menu



Pull-Down Menu

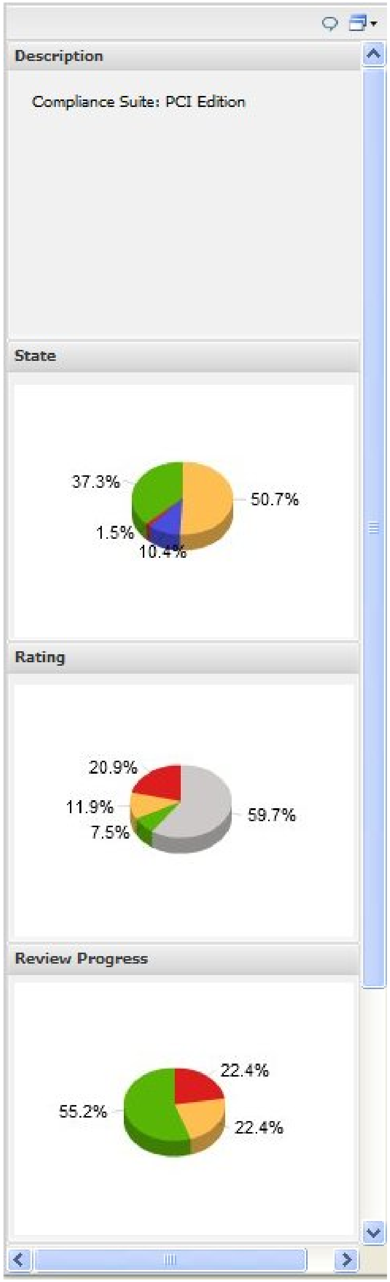
The **left** panel of the Audit Dashboard displays visual representations of report statistics per mandate for a selected period.

Audit Dashboard Left Panel

Icon	Description
	Click this button to add a comment to the selected mandate. The **Mandate Comment** text box appears. Type your comment and click **Save comment**. Comments appear in the **Review History/Comments** tab.

Icon	Description
	Click this button to display the list of panes that can be displayed in the Audit Dashboard left panel. Select or clear the relevant check boxes to show or hide these panes in the left panel.
Pane	**Description**
Description	Shows the mandate description.
State	Shows a pie chart with the current state of report reviews, i.e., reports which are ready for review, in review, complete, autocomplete or returned for the selected control.
Rating	Shows a pie chart with the ratings currently assigned to the reports for the selected control.
Review Progress	Shows a pie chart with the overall review progress, i.e., report reviews that are ontime, approaching due date or past due date
Review Progress Trend	Shows a stacked bar chart with the users' Review Progresss over a selected period, where: • x = day of the selected period • y = number of generated reports • z (color) = review progress proportion

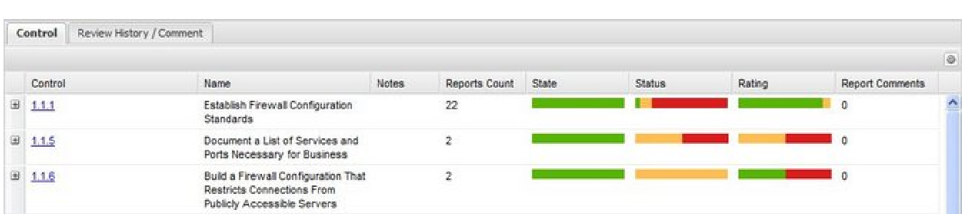
Audit Dashboard Left Panel



Control Tab

The **Control** tab displays a table listing all the controls related to the selected mandate

Audit Dashboard Control Tab



Audit Dashboard Control Tab

Button	Description
	Clears all filter conditions applied to the **Control** panel columns.
Column	Description
Control	Displays a link allowing to drill-down from the selected control to its associated reports.
Name	Displays the Control name
Notes	Control annotations (if any) are flagged by a comment icon
Reports count	Indicates the number of available reports retrieved from the appliance(s) for this control.
State	Indicates the ratio of the review states associated to the reports gathered in the control. The color code is the following: • Ready for Review • In Review • Returned • Complete
Status	Indicates the ratio of the review statuses associated to the reports gathered in the control. The color code is the following: • On time: The reports are on-time regarding the review due date. • Approaching due date: The report review is very close to the due date. The default time allowed before a review is given a yellow status is 80% of the elapsed time between the Creation date and the Due date. This threshold can be changed in *General Settings*. • Past due date: The report reviews are over the due date.
Rating	Indicates the ratio of the various ratings associated to the reports gathered in the control. The color code is the following: • No rating (no impact) • Low (minimal impact) • Medium (some impact) • High (High impact = High Risk)

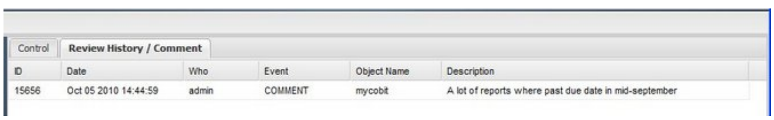
Button	Description
Report comments	Indicates the number of reports with annotations currently associated to the control. The hyperlink allows to open the control holding these comments.

Review History and Comments Tab

All events associated with a compliance report that is scheduled and assigned for review are recorded to meet the compliance activity documentation requirements of an audit. You can review the life cycle of a compliance report from the time of creation to completion in the **Review History & Comments** Tab

A list of events are recorded and time stamped when the report results were retrieved from the Appliance and the review entry was created, anytime the report state is changed by a Reviewer or Administrator (for example, when the report is Claimed, Returned, or Approved), or any comments added by a Reviewer, an Executive or an Administrator.

Audit Dashboard Review History & Comments Tab



Audit Dashboard Review History & Comments Tab

Column	Description
ID	Indicates the ID of the event
Date	Indicates the date when the action/comment was performed.
Who	Indicates the login name of the user who made the action/comment.
Event	Indicates the type of event that was performed that is an action such as create, add, remove, change; or an annotation such as comment, note.
Object Name	Indicates the name of the object on which the action /comment was made.
Description	Gives a description of the action/comment.

Tips About Columns in the Audit Dashboard Tables

- To sort a column by ascending or descending order, click once on its column header.
- To rearrange the order/position of columns, drag-and-drop column headers on the column header row.
- To select the columns that you want to display, click the down triangle arrow on the right hand side of any column header, select the Columns menu and tick their corresponding check boxes.
- To resize columns to the desired width, mouseover their column dividers and click-and-drag the left/right arrow.

Drilling-Down to the Report Definition Level

Control Points usually have many associated report definitions. The auditor can see all the report definitions related to a given control point for a given period, that is to say drill-down to the report definition level, via the **Control** tab of the **Audit** dashboard.

Drill-down actions depend on the appliance load and might therefore be very long (and sometimes fall in timeout). Obviously, the more powerful the hardware the faster the performances.

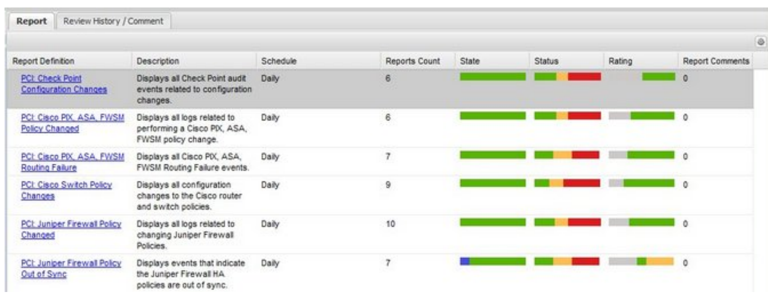
Procedure

1. Select the **Control** tab in the **Audit** dashboard.
   The **Control** column displays a link allowing to see the report definitions related to the selected control.
2. Click the **<control name>** link.

   The **Control** tab gives way to a **Report** tab listing all related summary report definitions.

   You can roll-up to the Control level (i.e. to the **Control** tab) by clicking the **<mandate name> link>** in the Audit dashboard header.

   Audit Dashboard Report Tab



Audit Dashboard Report Tab

Column	Description
Report Definition	Displays a link allowing to open the selected report definition and view its associated reports (its occurrences) in a **Reports for Review** tab.
Description	Displays the report definition description as shown in **Review Management > Map Reports to Control**
Schedule	Indicates the current schedule frequency of the report definition. It can be: • Daily at <HH:mm> • Weekly on <day of the week> • Monthly on day <#>
Reports count	Indicates the number of available reports retrieved from the appliance(s) for this report definition.

Column	Description
State	Indicates the review states associated to the reports generated for a report definition. The color code is the following: • Ready for Review • In Review • Returned • Complete
Status	Indicates the review statuses associated to the reports generated for a report definition. The color code is the following: • On time: The report review is on-time regarding the due date. • Approaching due date: The report review is very close to the due date. The default time allowed before a review is given a yellow status is 80% of the elapsed time between the Creation date and the Due date. This threshold can be changed in *General Settings*. • Past due date: The report review is over the due date.
Rating	Indicates the ratings associated to the reports generated for a report definition. The color code is the following: • No rating (no impact) • Low (minimal impact) • Medium (some impact) • High (High impact = High Risk)
Report comments	Indicates the number of comments made for the report definition.

Drilling-Down to the Report Results Level

You can also drill-down further than the report definition level and get to the report results level of a given report.

Drill-down actions depend on the appliance load and might therefore be very long (and sometimes fall in timeout). Obviously, the more powerful the hardware the faster the performances.

Procedure

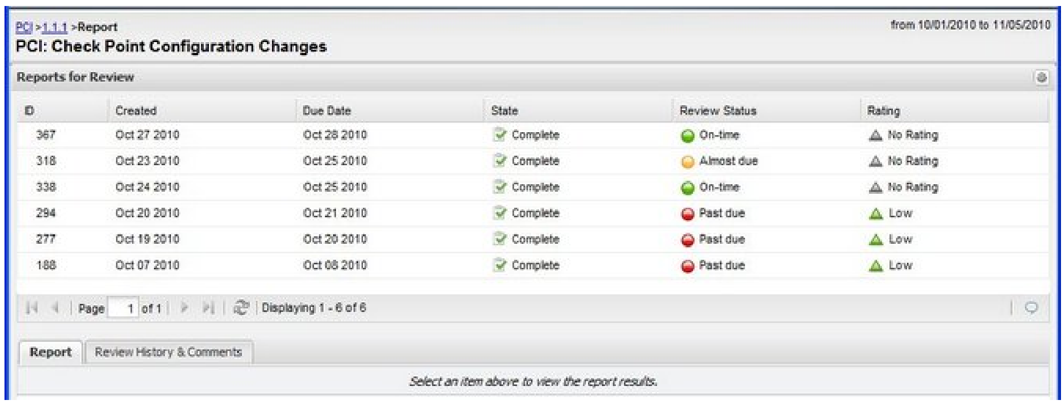
- Once you have drilled-down to the report definition level (see Drilling-Down to the Report Definition Level), click a link in the **Report definition** column.

The **Reports for Review** panel opens, listing all the reports generated for the selected report definition. It provides evidence on the review activities

When a report is selected, its results are displayed in the **Report** tab at the bottom of the screen.

> You can roll-up to the Report definition level (i.e. to the **Report** tab) by clicking the <control name> link> in the Audit dashboard upper bar.

Audit Dashboard Reports for Review Panel



Audit Dashboard Reports for Review Panel

Column	Description
ID	The numbered ID of the report result
Source Appliance	Indicates the name of the appliance where the report result were retrieved.
Created	The date the report result was queried and retrieved from the LogLogic Appliance
Due Date	The date the report must be completed by.
State	The current state of the report review: • Ready for Review • In Review • Returned • Complete

Column	Description
Review Status	The review status signifies the current state of the report along with the state of the review process. • On time: The report review is on-time regarding the due date. • Approaching due date: The report review is very close to the due date. The default time allowed before a review is given a yellow status is 80% of the elapsed time between the Creation date and the Due date. This threshold can be changed in *General Settings*. • Past due date: The report review is over the due date.
Rating	This attribute of a report review activity is specified by the reviewer. The four states are: • No rating (no impact) • Low (minimal impact) • Medium (some impact) • High (High impact = High Risk) **Note:** The definition of Rating should be determined by your Compliance process and how you choose to interpret this value in Summary results.

Monitoring Report Results

The **Report** tab contains a table displaying the results of the report selected above, in the **Reports for Review** panel. These report results can be considered as summary views of similar report rows. You will moreover see that many reports display a **Count** column to indicate precisely the number of rows corresponding to each report result. The count hyperlink allows to drill-down to the report rows, that is to say to the **Report Result Details** level.

Contents

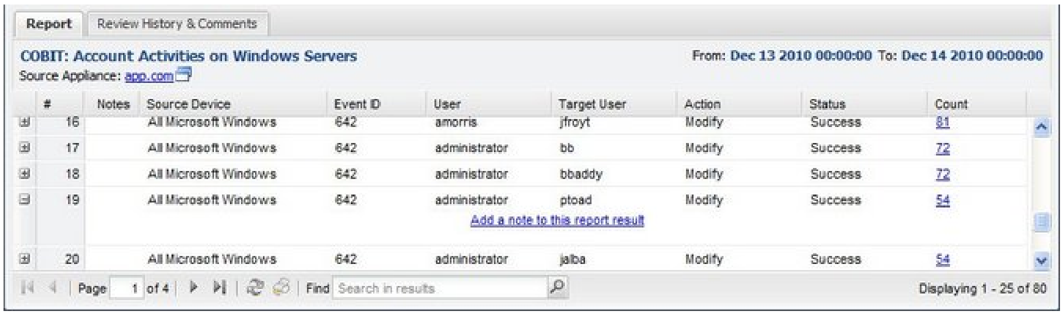
Adding/Viewing Report Result Annotations

Each result in a report can contain one or multiple annotations, or notes. You can do a fine-grain commenting of the report, down to the report result level. Report result annotations are archived and can be edited or deleted once created.

Procedure

1. Select a Report in the **Reports for Review** list.
2. Double-click a report result in the **Report** tab to expand it.

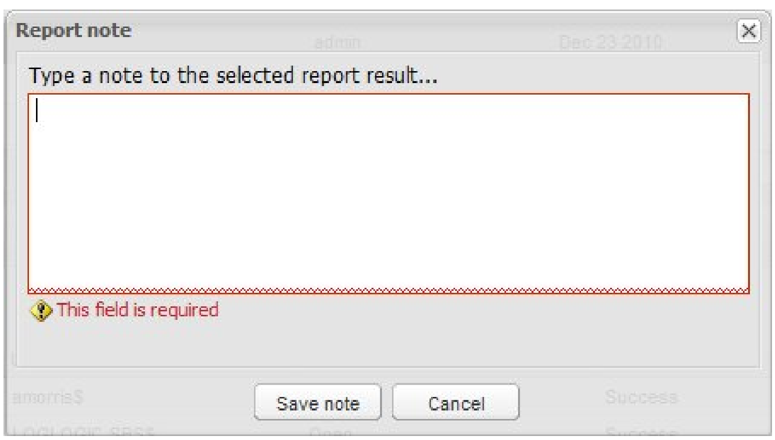
   Add a Note to this Report Result Link



3. Click the **Add a note to this report result** link.

   The **Report note** dialog box opens.

   Report note Dialog Box

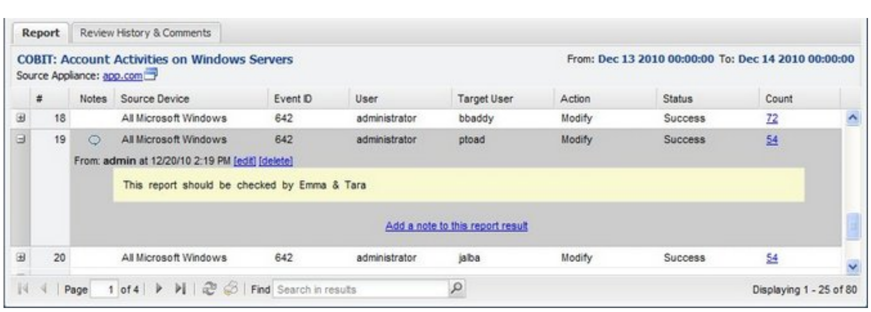


4. Type in your comment and click **Save note**.

   The Annotation is displayed below the report result with the timestamp of when the Annotation was created, and the User Account that created the Annotation.

   The report results that have an annotation, display an icon in the **Notes** column. Double-click the report result to display all its annotations.

   Display of Report Result Annotation

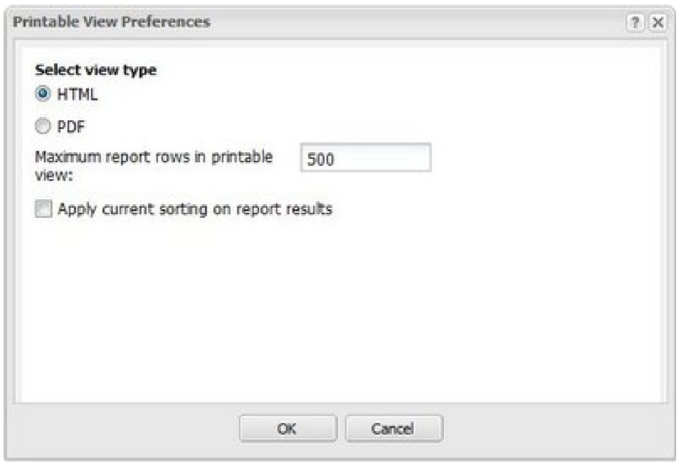


The report result note can be edited or deleted by clicking the [Edit]/[Delete] links.

Printing Report Results

Procedure

1. Click the **printer** icon located at the bottom of **Report** tab.
   The **Printable View Preferences** window opens.
   Report Results Printable View Preferences



2. In the **Printable View Preferences** window, set the Print settings as needed.

   Printable View Preferences

Setting	Description
HTML/PDF	Use these radio buttons to select the file format for the printable view, i.e., either **HTML** or **PDF**
Maximum report rows in printable view	Enter the maximum number of report rows that must be displayed in the printable view.
Apply current sorting on reports	Tick this check box if you want your report to reflect your sorting preferences.

3. Click **OK**.

   The report review is generated in the format you selected, i.e. HTML or PDF, suitable for sending to a printer or downloading for reviewing offline. The HTML and PDF versions contain the following information:

   - Report Name
   - Retrieval Time
   - Due Date
   - Name of the Current Reviewer
   - Source Appliance for the Report
   - Description of the report
   - List of controls the report addresses
   - List of Report History and Comment Events

- Report Results including annotations

Drilling-Down to the Report Result Details Level

For the reports displaying a **Count** column, it is possible to drill-down to the **Report Result Details** level and see all the rows corresponding to each report result.

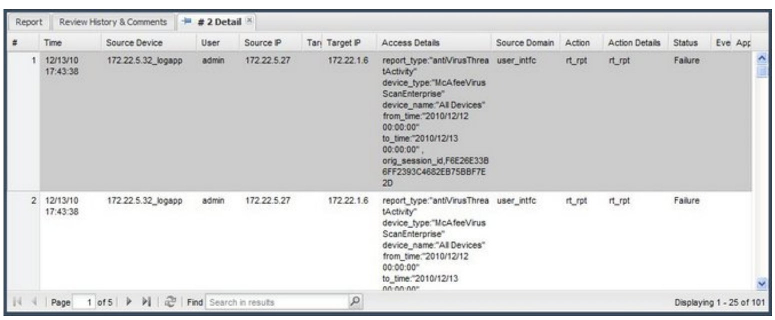
Drill-down actions depend on the appliance load and might therefore be very long (and sometimes fall in timeout). Obviously, the more powerful the hardware the faster the performances.

Procedure

1. In the **Count** column of the **Report** tab, click the hyperlink of a report result.

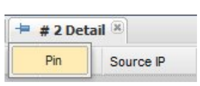
   A new tab appears in the bottom panel. Its label displays the line number of the report result (the format is # **<line number> Detail**) as shown in the **Report** tab. The generation of the report result details can take a few minutes.

   Report Result Details Tab

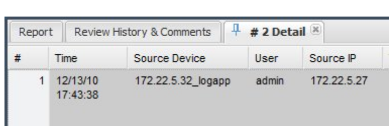
2. To save the report result detail tab for future use, mouseover the tab label and click **Pin** in the pop-up menu

   Report Result Detail Tab Pin Option

   Once pinned, the report result detail tab will always be displayed in the bottom panel of the Review dashboard when you select the same report in the **Reports for Review** panel

   Pinned Report Result Detail Tab

3. You can repeat the three first steps to open and pin more report result detail tabs.

   If you want to unpin a tab, mouseover its tab label and click **Unpin** in the the pop-up menu.

   All data of drill-down actions will be deleted from the CM database every 24 hours unless report result detail tabs are pinned.

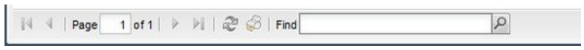
Searching in the Report tab

Use the **Find** box at the bottom of the panel to quickly filter the report results.

Procedure

1. Enter text into the **Find** box

Report tab Find Box



2. Press **Enter**.

   The view will be filtered to display only the results containing the matching text (this text highlighted in bold characters).

Consulting the Review History & Comments

To view the change history and comment of a report review listed in the **Review Dashboard**, select it and consult the list displayed in the **Review History & Comments** tab.

Managing Report Reviews

Review Management is where LogLogic® Compliance Manager Administrators can manage out of the box and custom mandates, map reports to controls, schedule reports, and manage report reviews to respond to their organizations' compliance project scope.

The **Review Management** menu is available only to user accounts with Administrator role.

Contents

Mandate Management

In **Review Management** > **Mandate Management** , the CM administrator or the Project Manager can customize the out of the box CM mandates and add their own enterprise regulations as mandates in LogLogic® Compliance Manager.

Contents

Description of the Mandate Management Workspace

The Mandate Management workspace is split into two panels:

- The **Mandates** panel (on the left) displays a tree list of the existing mandates and a tool bar allowing to add, duplicate and remove items.

  Mandates Panel Description

Element/Icon	Description
Add Mandate	Creates a new mandate node (branch) in the tree list
Add Control	Creates a new control node (leaf) within a selected mandate node in the tree list
Duplicate	Creates either a new branch or leaf node depending on the current GUI selection, i.e., mandate or control.
Remove	Removes the selected node(s) from the tree list

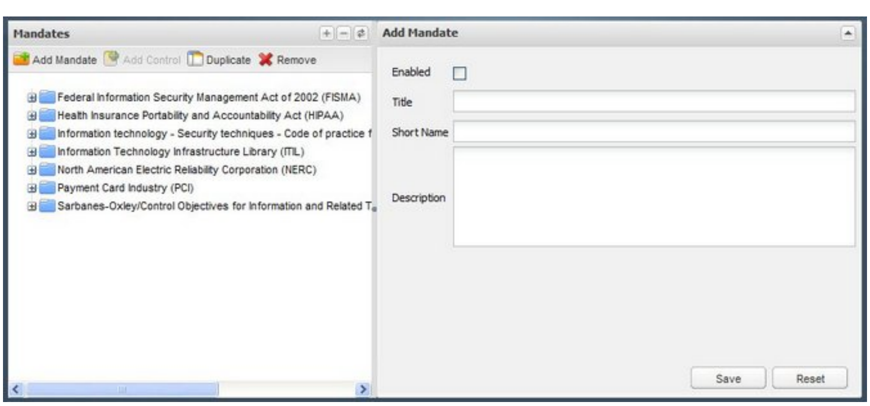
Element/Icon	Description
	Represents an enabled out of the box mandate.
	Represents an enabled control contained in an out of the box mandate.
	Represents an enabled custom mandate.
	Represents an enabled custom control contained in a custom mandate.
	Represents a disabled mandate.
	Represents a disabled control

- The right panel displays the properties of the selected mandate or control.

Add Mandate/Control Panel Description

Element/Icon	Description
Enabled	Indicates whether the selected mandate or control is enabled or not. When disabled, the mandate or control icon is grayed out.
Title	Indicates the title of the selected mandate or control. The maximum number of characters is 255 and the minimum number is 1.
Short Name	Indicates the short name of the selected mandate or control. The maximum number of characters is 255 and the minimum number is 1.
Description	Displays a description of the selected mandate or control

Mandate Management Workspace



Adding Custom Mandates and Controls

LogLogic® Compliance Manager allows you to create your own custom mandates and its associated controls in a few clicks. You then only have to map report definitions to controls in **Review Management** > **Map Reports** to Controls.

- Adding Custom Mandates
- Adding Custom Controls

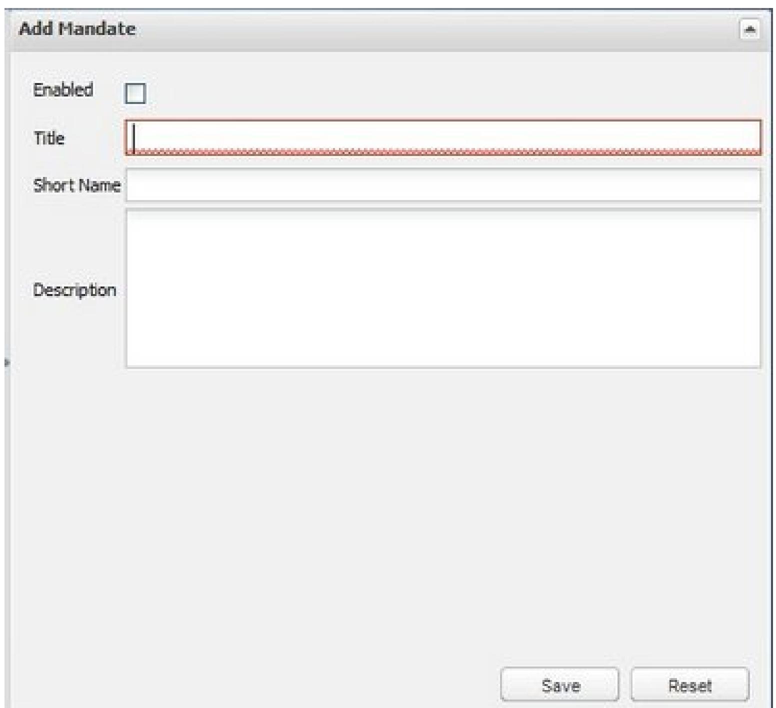
Adding Custom Mandates

Procedure

1. Click the **Add Mandate** button in the Mandates panel.

   The **Add Mandate** panel opens

   Add Mandate Panel

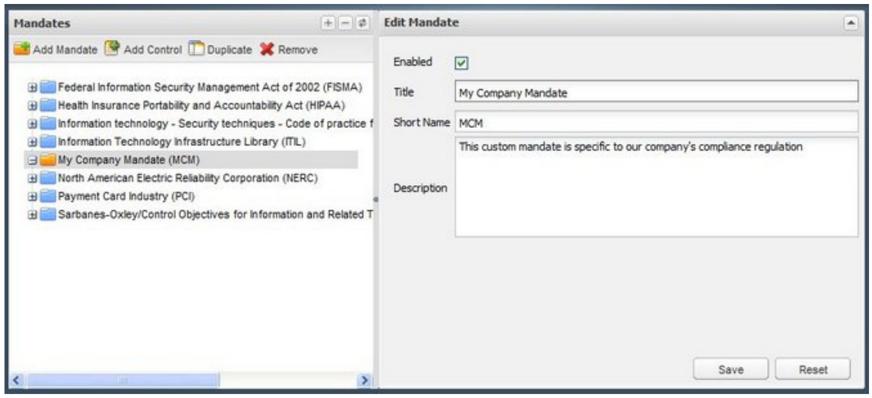
   

2. Type in a title, a short name (max. number of characters = 255, min. = 1), and a description for the new mandate.
3. Tick the **Enabled** check box if you want to activate the mandate.
4. Click the **Save** button.

   A pop-up dialog box prompts that the mandate has been saved.

   The new mandate is displayed at the bottom of the tree list in the **Mandates** panel and the **Add Mandate** panel changes to **Edit Mandate**.

New Custom Mandate Created



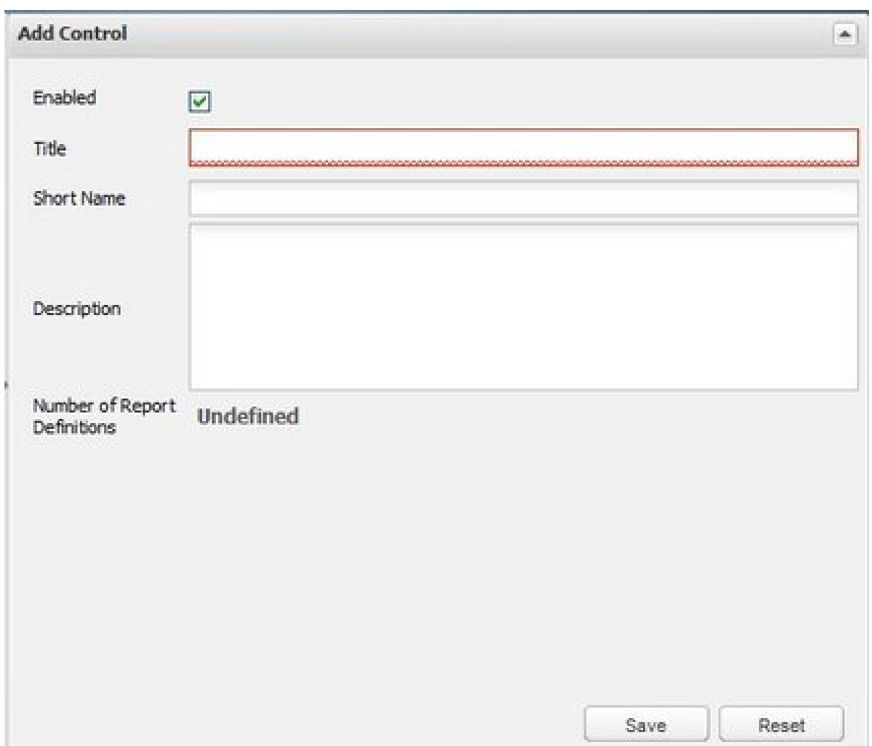
Adding Custom Controls

Procedure

1. Select a custom mandate in the Mandates panel and click the Add Control button.

   The Add Control panel opens

   Add Control Panel

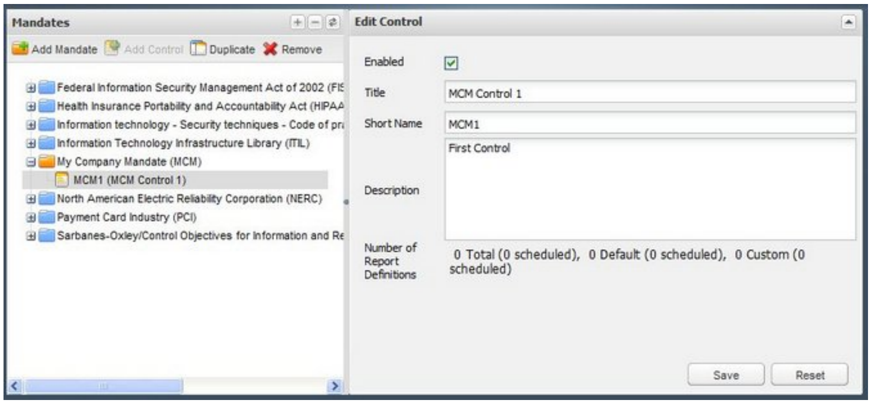


2. Type in a title, a short name (max. number of characters = 255, min. = 1), and a description for the new control (the **Enabled** check box is selected by default).
3. Click the **Save** button.

   A pop-up dialog box prompts that the control has been saved.

   The new control is displayed as a leaf node of the selected mandate in the **Mandates** panel, and the **Add Control** panel changes to **Edit Control**.

New Custom Control Created



4. You now have to link report definitions to the newly created control. This can be done in **Review Management** > **Map Reports** to Controls. See Map Reports to Controls.

Duplicating Mandates and Controls

The Duplicate functionality allows you to copy either a branch or a leaf in the list depending on the selected node, that is to say:

- an out of the box or a custom mandate with all their associated controls.
- an out of the box or a custom control.

The name of the duplicated node is the `<original name>` appended by `_copy#`

The digit `#` will be incremented if the node is duplicated.

Example of Duplicated Mandate

Please also note that:

- The newly created node is enabled by default.
- The controls in a duplicated mandate keep their original names.
- The associated reports will be kept for the duplicated node.
- The reports schedules are kept but disabled for the duplicated node.
- The user associations are NOT kept for a duplicated mandate (go to **Administration** > **User Management** to assign the duplicated mandate to users).

Removing Mandates and Controls

The Remove functionality allows you to remove either a branch or a leaf in the list depending on the selected node, that is to say:

- a custom mandate with all its associated controls.
- a custom control.

Please note that:

- The scheduled tasks associated to the deleted node are also deleted.
- The review tasks in "Ready for review" state associated to the deleted node are also deleted.
- The review tasks in "In review", "Returned" or "Complete" state are kept (for statistics usage).

Map Reports to Controls

In **Review Management** > **Map Reports to Controls** , the CM administrator can map previously imported custom report definitions to the controls of compliance Mandates. The default report definitions present in the Compliance suites are automatically mapped.

Contents:

Process Overview

Before mapping report definitions to controls the CM administrator must perform the following steps:

If you are working only with the report definitions that are part of the out of the box suites (PCI, SOX, ITIL, FISMA, HIPAA, COBIT, NERC) these report definitions are already mapped; you can skip this step.

Once report definitons are mapped to controls, the CM administrator can schedule the retrieval of reports from the appliance(s) in **Review Management** > **Schedule Reports**.

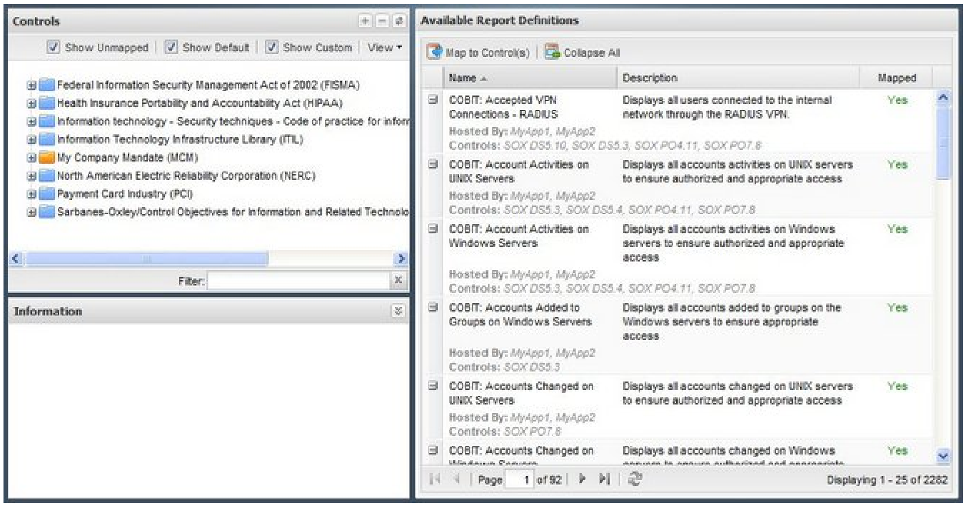
Procedure

1. Add an appliance by going to **Administration** > **Appliances**. This allows report definitions from an existing LogLogic appliance (LX/MX/ST) to be managed via CM. 2
2. Retrieve report definitions from the appliance(s) by going to **Administration** > **Appliances**and clicking . This will bring in all the report definitions from the appliance.

Description of the Map Reports to Controls View

The Map Reports to Controls view displays 3 panels, i.e., **Available Report Definitions**, **Controls** and **Control/Mandate Description**.

Map Reports to Controls View



Available Report Definitions Panel

The panel on the right, **Available Report Definitions**, displays the current inventory of report definitions retrieved from appliances (defined in **Administration** > **Appliances**). These report definitions can either be already mapped to controls (i.e. for the controls of default mandates) or unmapped, in which case you must map them to default or custom controls.

Available Report Definitions Panel Description

Icon	Description
Map to Control(s)	Allows to map a selection of report definitions in the **Available Report Definitions** panel with a specific Control in the Controls panel
Collapse All/Expand All	Allows to collapse or expand all rows in the **Available Report Definitions** panel.
Column	Description
ID	The ID number of the report definition (generated by LogLogic® Compliance Manager).
Name	The name of the report definition as defined by the LX/ST/MX.
Description	The description of the report definition as defined by the LX/ST/MX.
Mapped	Yes, if the report definition is mapped to at least one Control, otherwise the value is No.
Other Information	Description
Hosted by	The list of appliances where the report definition is available (only shown when the row is expanded).
Controls	The list of Controls the report definition currently maps to (only shown when the row is expanded).

Current Reviewer	The reviewer of the report definition.

Column Tips

- To sort a column by ascending or descending order, click once on its column header. Sorted columns have a dark grey header and their names are followed either by an upward (ascending) or a downward (descending) arrow.
- To rearrange the order/position of columns, drag-and-drop column headers on the column header row.
- To select the columns that you want to display, click the down triangle arrow on the right hand side of any column header, select the Columns menu and tick their corresponding check boxes.
- To resize columns to the desired width, mouseover their column dividers and click-and-drag the left/right arrow.

Controls Panel

The panel on the left, Controls, displays a tree list which shows the available controls and their associated mapped report definitions.

Element	Description
Show Unmapped	Tick this check box to view all unmapped control nodes in the tree list.
Show Default	Tick this check box to view all default report definitions in the tree list.
Show Custom	Tick this check box to view your custom report definitions in the tree list.
View	Click this pull-down menu to select which report definitions to display in the tree list, i.e., All, Scheduled, or Unscheduled reports.
<mandate> tree <mandate> tree	list The tree list of the Controls panel displays the default and the custom mandates (if any) defined in CM. Each mandate contains a list of controls which themselves contain report definitions.
Filter	Type in a text in this text entry box to filter the list of Controls. This text entry box is not case-sensitive.

Mandate/Control Description Panel

The **Mandate/Control Description** panel shows information relative to the Mandate/ Control selected in the tree list of the **Controls** panel:

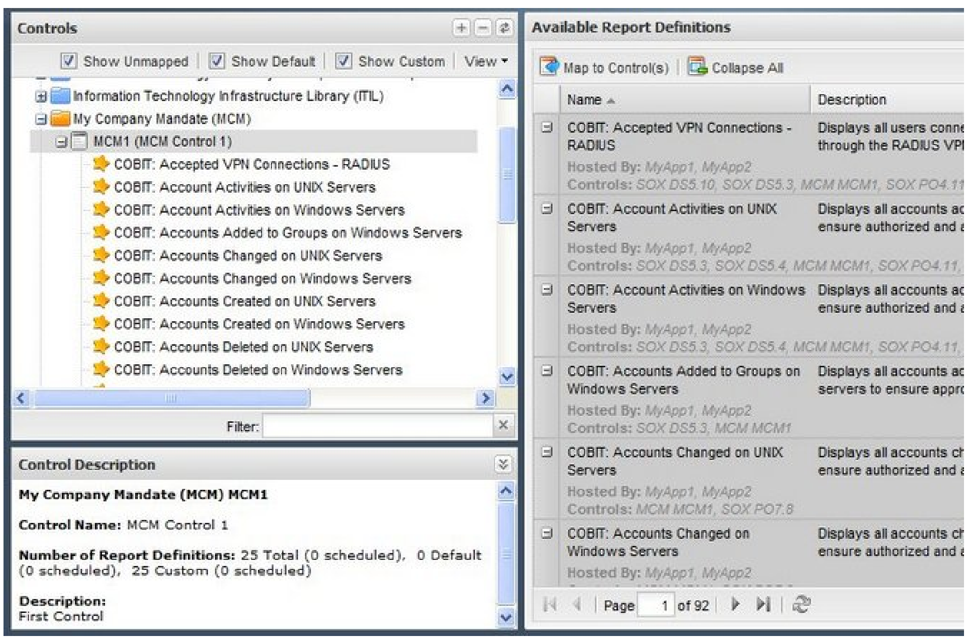
- The total number of report definitions available and the number of scheduled reports.
- The number of default report definitions and the number of scheduled reports for these.
- The number of custom report definitions and the number of scheduled reports for these.
- The description of the Mandate/Control.

Adding a Report Definition/Control Association

Procedure

1. Select one or more controls in the **Controls** panel.
2. Select one or more report definitions in the **Available Report Definitions** panel.
3. Click the **Map to Control(s)** button in the **Available Report Definitions** Panel. The selected report definition(s) is listed within the selected Control folders in the **Controls** panel. It is preceded by a yellow star  .

   Report Definition Mapped to Selected Control



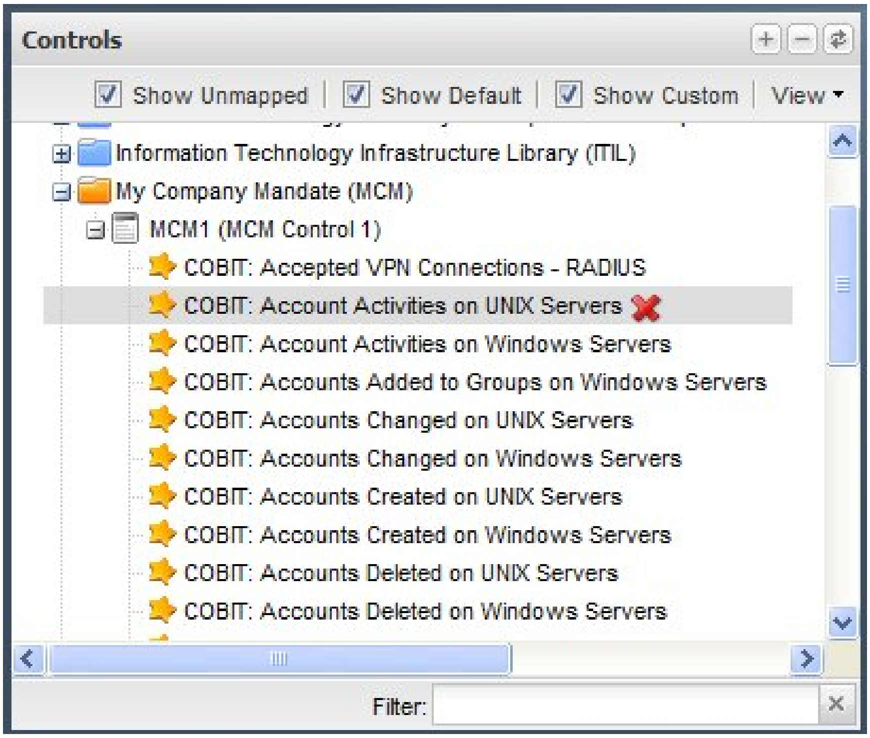
Removing a Report Definition/Control Association

Procedure

1. Select a report definition in the **Controls** panel.

   The report definition is highlighted and a remove button is displayed at the end of the line.

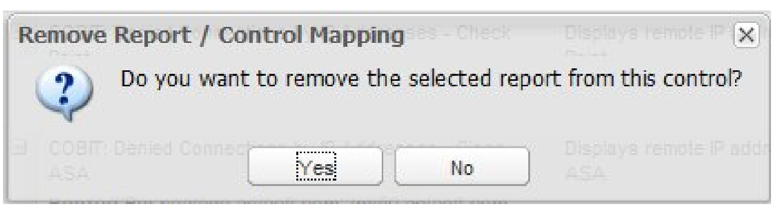
Select a report definition in the Controls panel.



2. Click the **Remove** button.

   A **Remove Report/Control Mapping** dialog box opens asking you to validate the unmapping.

   Remove Report/Control Mapping Dialog Box



3. Click **Yes** to validate.

   The report definition is moved from its control folder (in the Controls panel) to the list of report definitions in the **Available Report Definitions** panel.

Schedule Reports

In **Review Management** > **Schedule Reports**, the CM administrator can enable, disable, and edit schedules for reports.

- How Are Report Schedules Performed?
- Description of the Report Schedule View
- Adding/Editing a Report Schedule
- Adding/Editing Several Report Schedules at Once
- Changing Reviewers for a Report
- Viewing Information for Mandate/Control/Report
- Viewing/Filtering the Display of Report Definitions

How Are Report Schedules Performed?

- Report Schedule Process Description
- Report Schedule Definition

Report Schedule Process Description

Before detailing how to create a Report Schedule in CM, it is essential to understand how report schedules are performed by the application.

A report schedule can be compared to a task generator. Each generated task contains a schedule phase and a review phase.

During the schedule phase, a report query is sent on one or several appliances to retrieve LMI report data at a precise time of the day*, depending on a query time range. The query time range can have a Daily, a Weekly or a Monthly frequency and always ends at midnight on the day that precedes the schedule phase. The aim of this schedule mechanism is therefore to retrieve report data on a continuous way even if its retrieval relies on segmented query time ranges.

* (The task may not be executed at that very precise time of the day because all tasks are scheduled at the same time and they are processed one after the other.)

Once the schedule phase is complete, the review phase begins. The report reviewers have to make a review of the report data retrieved during the schedule phase, respecting a due date.

For the same mapped report definition, there will be as many review tasks created as there are instances of this report definition on the appliances used by CM, and calls of this report definition in the CM Controls.

For example, if report definition A is:

- retrieved from Appliance 1 and Appliance 2
- and used in Control Y and Control Z
- then the schedule report process will generate 4 review tasks.

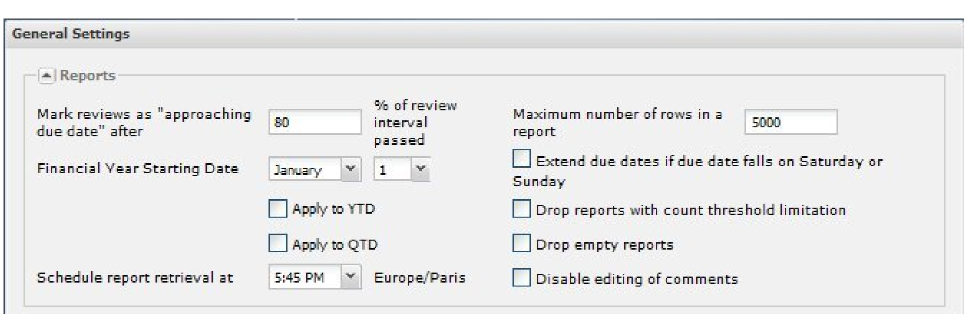
Report Schedule Definition

We now have to look concretely how report schedules are defined in CM.

Procedure

1. The precise of time of the day when the schedule phase is executed, is defined through the **Schedule report retrieval at** property in **Administration** > **General Settings**.

   Schedule Report Retrieval Property

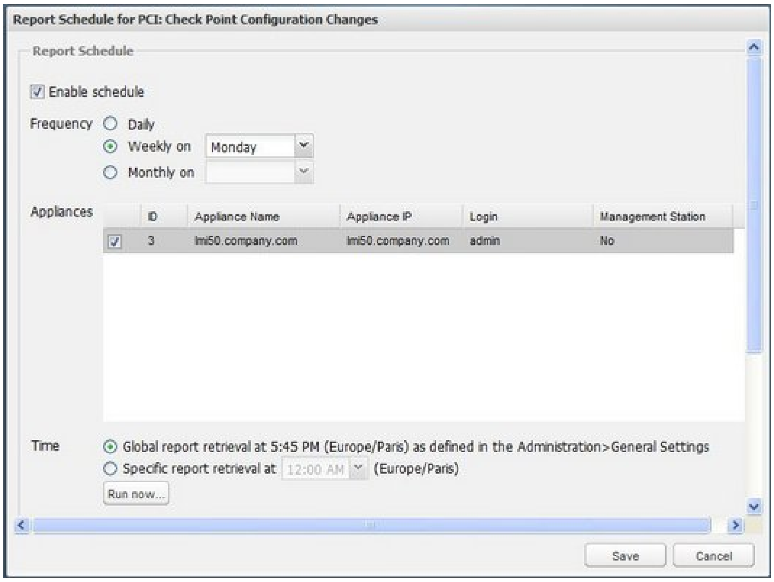
   

2. The frequency and the appliances on which data are retrieved, are defined in the **Report Schedule** pane of the **Report Schedule for <report name>** panel in **Review Management** > **Schedule Reports**.

The general schedule time defined in **Administration** > **General Settings** can be overloaded specifically report by report by selecting the **Specific report retrieval** radio button and selecting a specific time.

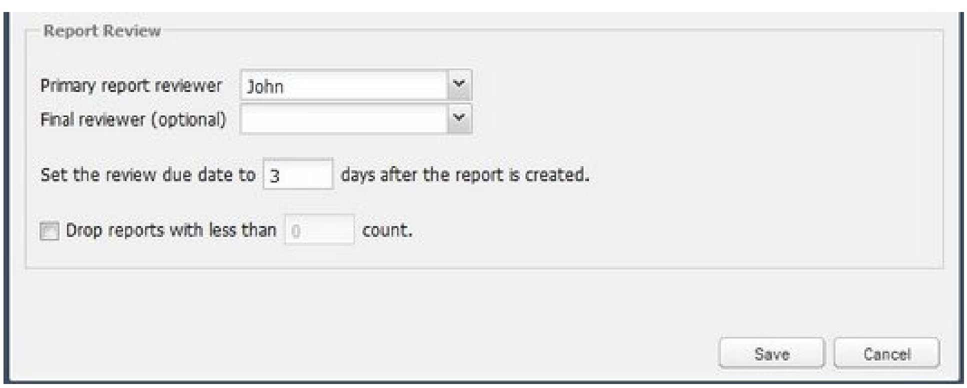
The **Run now** button can also be used if you want to execute the schedule immediately.

Report Schedule Panel: Report Schedule Pane



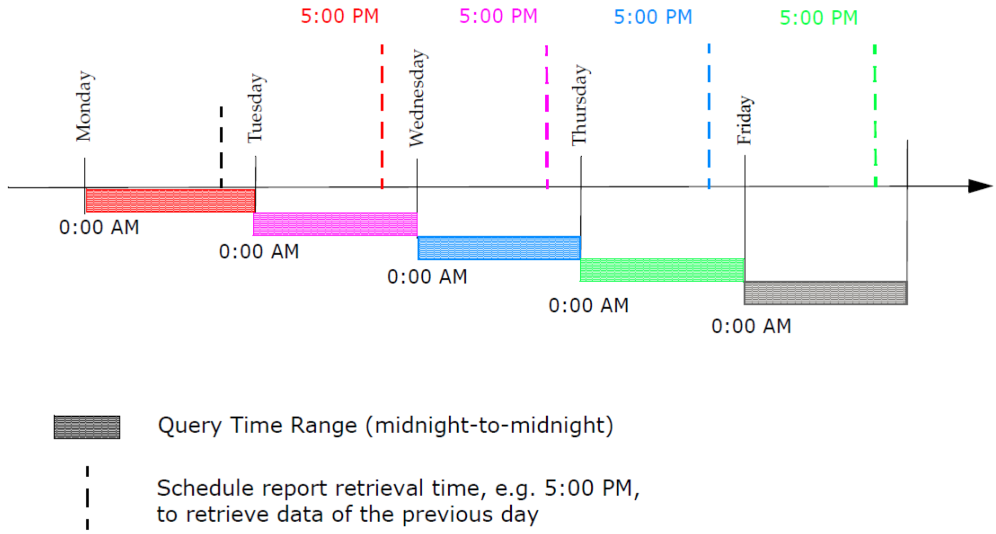
3. The parameters of the report review phase are defined in the **Report Review** pane of the **Report Schedule for <report name>** panel. Use the various properties to select reviewers and the review due date.

   Report Schedule Panel: Report Review Pane



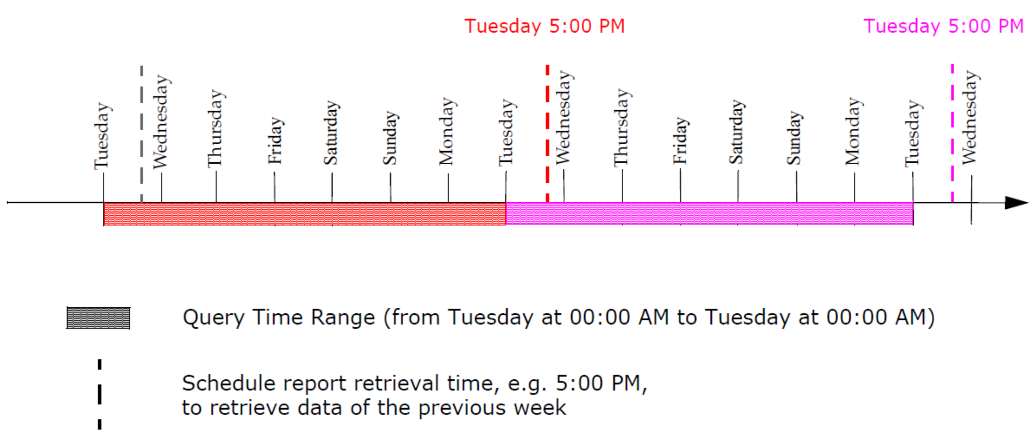
Example 1 Report Query with Daily Frequency

The graphic below shows a report query having a daily frequency. The schedule task which retrieves the report data of the previous day is set at 5:00 PM. Therefore, a new schedule task will be created and executed every day at 5:00 PM to retrieve the report data.



Example 2 Report Query with Weekly Frequency

The graphic below shows a report query having a weekly frequency. The schedule task which retrieves the report data of the previous week each Tuesday at 5:00 PM. Therefore, a new schedule task will be created and executed every Tuesday at 5:00 PM to retrieve the report data.

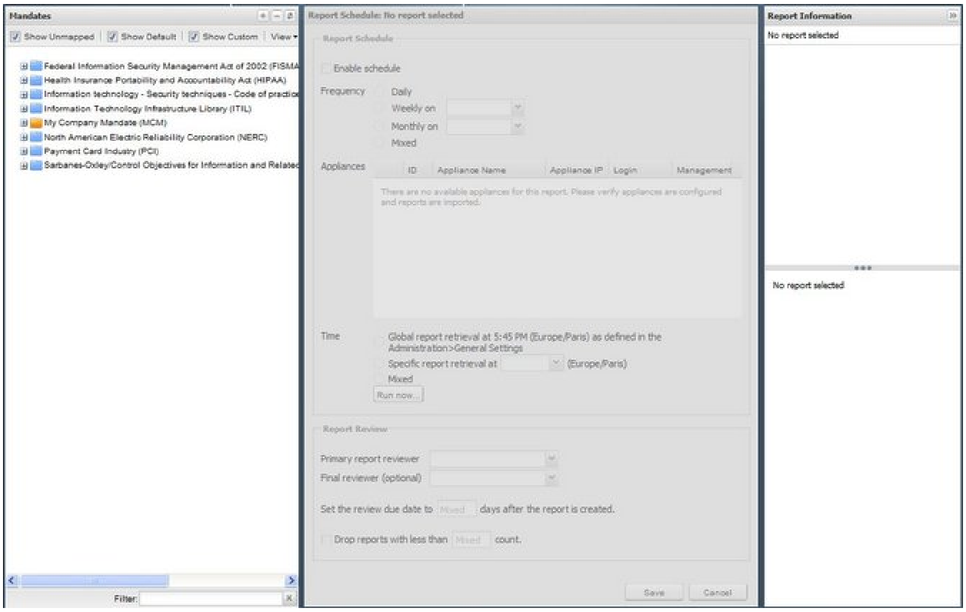


Description of the Report Schedule View

There are three panels in the Report Schedule view:

- **Mandates** which lists all the Compliance mandates and their associated controls
- **Report Schedule** where you enable, disable, and edit the report's schedule and Reviewers
- **Mandate/Control/Report Information** which displays information about the selected item.

Report Schedule View



Adding/Editing a Report Schedule

Procedure

1. Select a report from the **Mandates** panel.

   A **Report Schedule for <report name>** panel opens.

2. In the **Report Schedule** pane, configure the report schedule settings as described in the following table.

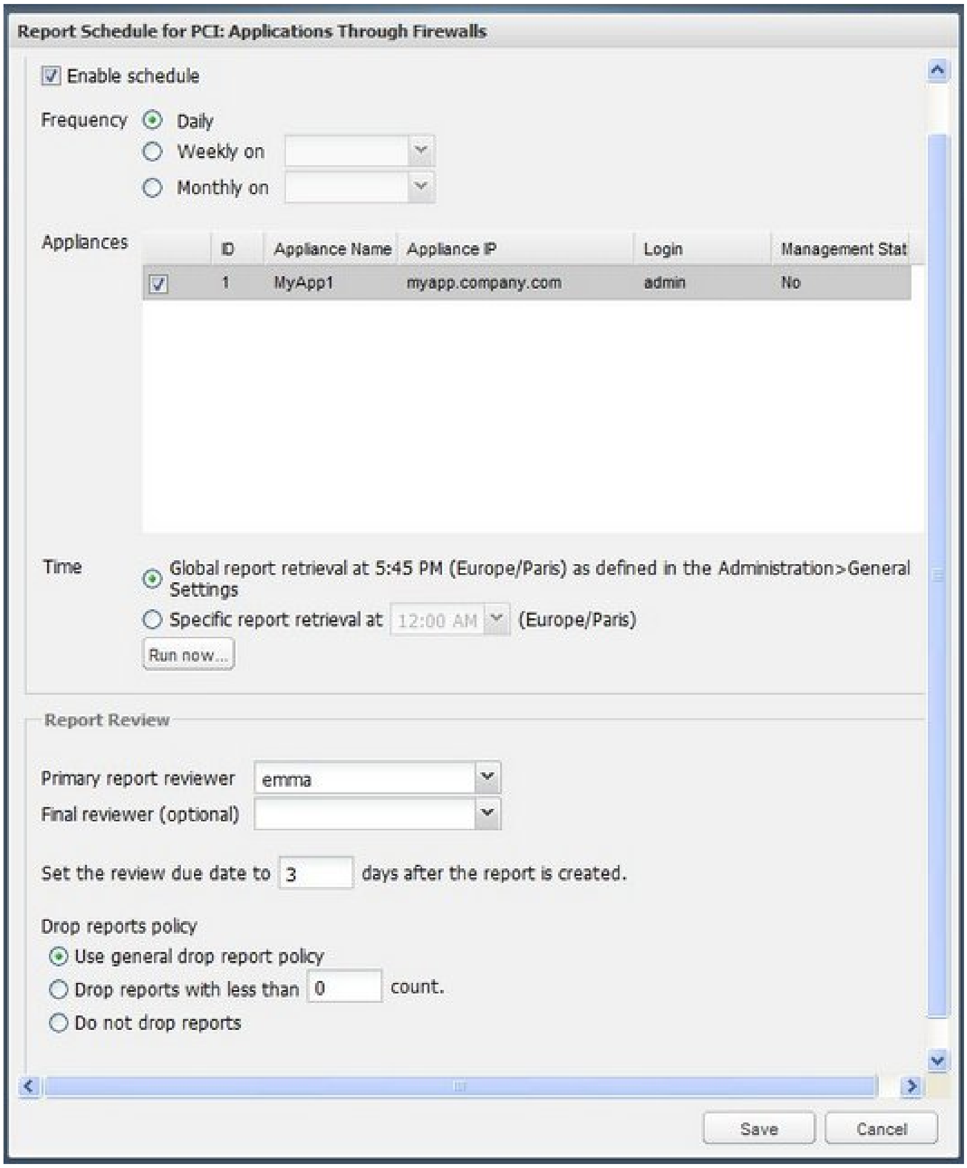
   Report Schedule Settings

Setting	Description
Enable schedule	Select whether to enable the report schedule or not.
Frequency	Select how often you want to run the report; Daily, Weekly, or Monthly
Appliances	Choose the appliances you want to run the report query on by enabling the check boxes in the ID column
Time	Choose when the report retrieval must be executed: • Global report retrieval at... is the report retrieval time as defined in the Administration > General Settings menu. • Specific report retrieval at... lets you select a specific report retrieval time that will overload the global setting. • Run now... allows you to launch the report retrieval at once.

3. In the **Report Review** pane, configure the report review settings as described in the following table.

Report Review Settings

Setting	Description
Primary report reviewer	Assign the primary report reviewer by selecting a name from the drop-down list
Final reviewer	Optionally, assign the final reviewer by selecting a name from the drop-down list
Set the review due date to [n] days after the report is created	Enter the number of days to allow for the Report Review
Use general drop report policy	Tick this radio button to use the general drop report policy defined in **Administration > General Settings** (in the Reports pane).
Drop reports with less than # count	Tick this radio button to drop the reports that will be sent for review if they have less counts than what is required in the **count** field.
Do not drop reports	Tick this radio button to if you do not want reports generated out of this scheduled report definition to be dropped.



4. Click **Save** to apply the settings to the report (or **Cancel** to clear them).

   The report is scheduled as defined. It is highlighted by a scheduled report icon in the tree list of the **Mandates** panel.

Adding/Editing Several Report Schedules at Once

You can add/edit several Report Schedules at once, by selecting reports in the **Mandates** panel using the Ctrl and SHIFT keys, and defining their schedules in the **Schedule for n Reports** panel as you would for a single report schedule (see Adding/Editing a Report Schedule).

Changing Reviewers for a Report

LogLogic® Compliance Manager uses the Report Schedule's **Final reviewer** setting to determine the next Reviewer assigned to the Report when the Primary reviewer approves the Report.

To change the Final reviewer for New or In-Review Reports, use the **Final reviewer** setting in the Report Schedule panel. LogLogic® Compliance Manager will use the new value when assigning the Final reviewer to reports in New or In-Review state.

For reports that are called in multiple controls, the assignment of a Final reviewer for a Report scheduled within a control will NOT be transmitted to all other controls.

The Reviewers (Primary or Final) can be changed for Complete reports.

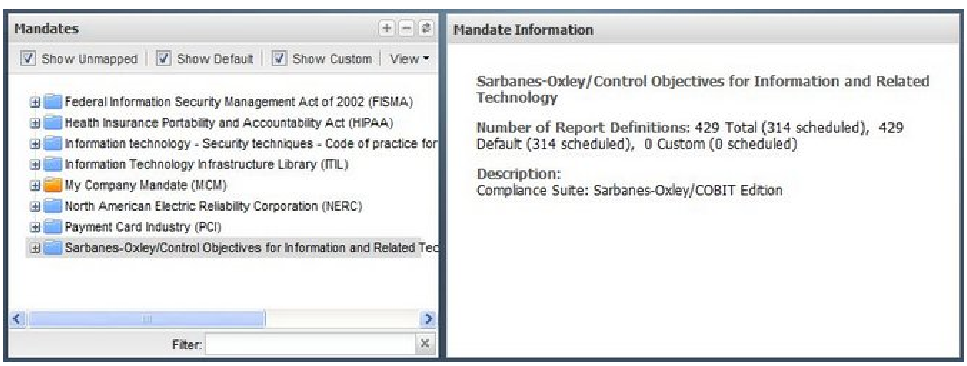
Viewing Information for Mandate/Control/Report

The Schedule Report view provides you with information relative to the type of element selected in the **Mandates** panel, that is to say about mandates, controls or report definitions.

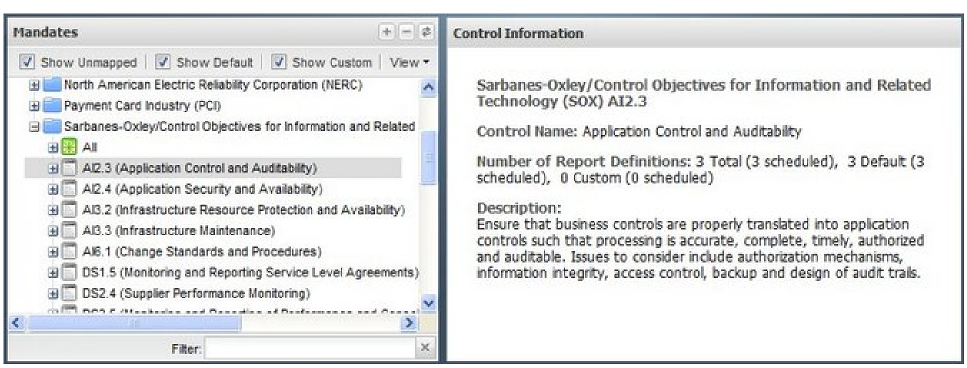
Procedure

1. If a mandate is selected, a **Mandate Information** panel displays the number of report definitions it contains and its description.
2. If a control is selected, a **Control Information** panel displays its name, the number of report definitions it contains and its description.
3. If a report defnition is selected, a **Report Information** panel displays the name of its parent mandate, the number of controls that use it (the current control is displayed in bold characters in the list, other controls are shown in regular characters). Moreover, a description of the report is displayed in the **Report Description** section.

Mandate Information Panel



Control Information Panel



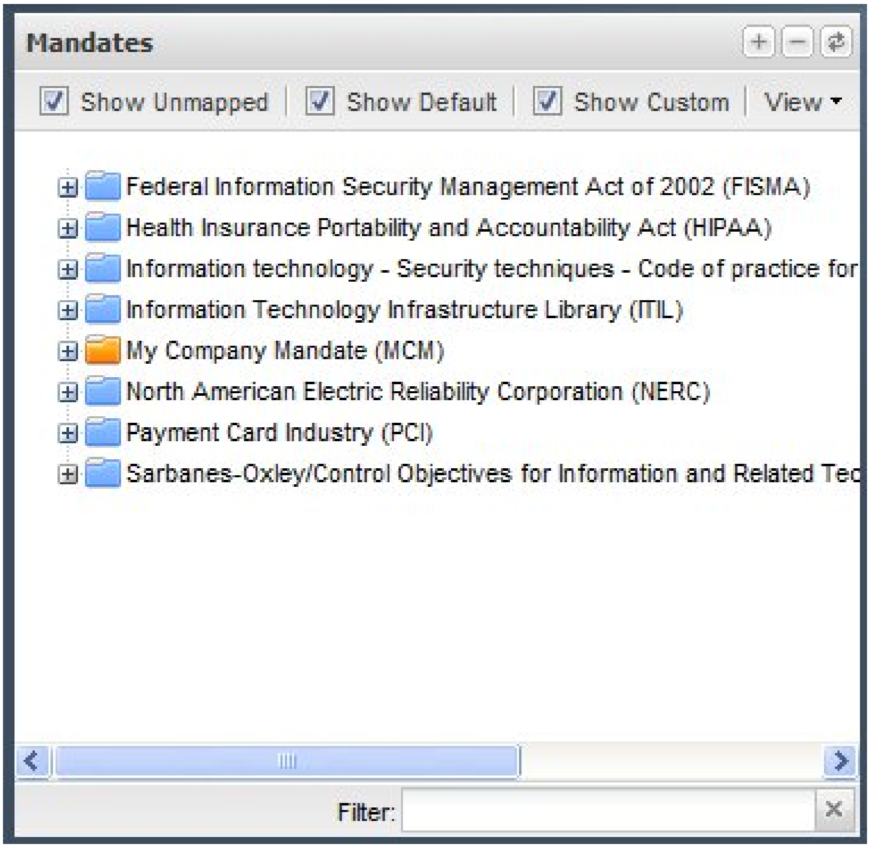
Report Information Panel

Viewing/Filtering the Display of Report Definitions

The display of report definitions can be tuned in the tree list of the **Mandates** panel using the toolbar at the top of the panel and the Filter text entry box at the bottom of the panel (see Figure 79):

- Tick the **Show Unmapped** check box if you want to view all the controls which do not have any report definitions (empty controls).
- Tick the **Show Default** check box if you want to view all default report definitions.
- Tick the **Show Custom** check box if you want to view your custom report definitions.
- Click **View** to select All, Scheduled, or Unscheduled report definitions.
- Type in a text in the Filter text entry box to filter the tree list. This text entry box is not case-sensitive.

View Report Check boxes



Manage Reviews

In **Review Management** > **Manage Reviews**, the CM administrator can view a collection of reviews, re-assign reviews, specify ad-hoc reviewers, extend due dates, change the state of the review, and change the rating.

The review settings defined in this view will determine the actions that users will have to perform in the **Dashboard** > **Review view**. See Review Dashboard for further information.

Contents:

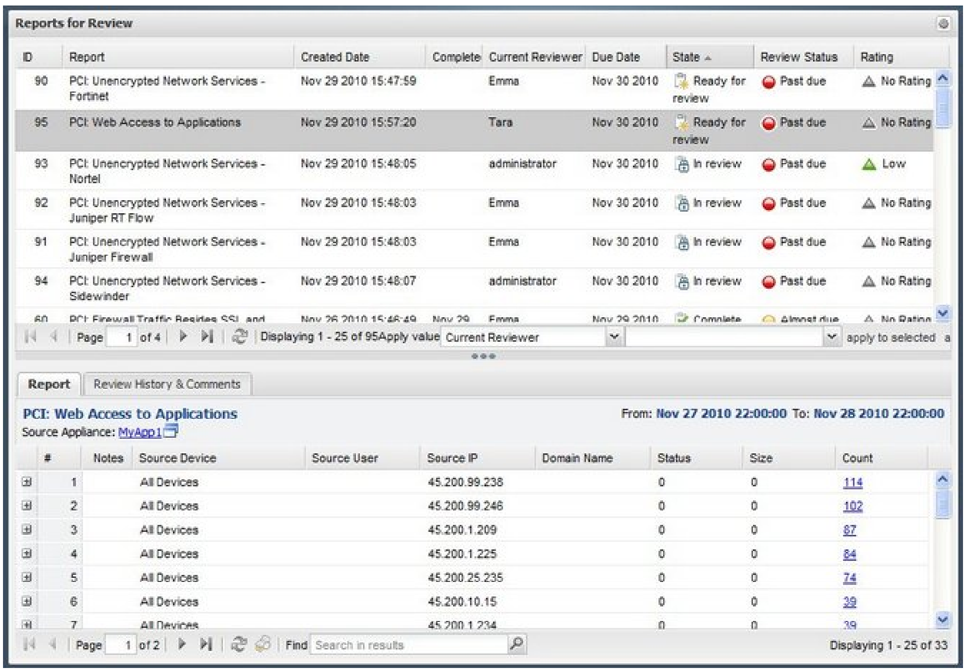
Description of Manage Reviews View

Reports for Review Panel

The **Reports for Review** panel lists all the reports that must be reviewed to provide the needed evidence that the log collection and review activities were completed and make an assessment about the compliance posture of the organization.

When a report is selected, its results are displayed in the **Report** tab at the bottom of the screen.

Report for Review Panel



Reports for Review Panel descriptions

Column	Description
ID	The numbered ID of the report results
Source Appliance	The appliance where the report results were retrieved from
Report	The name of the report
Created Date	The date the report results were queried and retrieved from the LogLogic Appliance
Completed Date	The completion date of the report
Current Reviewer	The reviewer of the report
Due Date	The date the report must be completed by

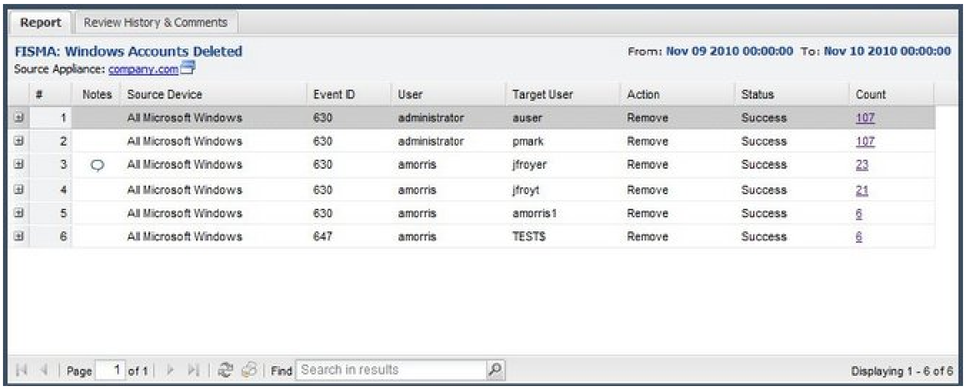
Column	Description
State	The current state of the report review: • Ready for Review : report has been retrieved from an appliance. • In Review: report has been claimed by a Reviewer. • Returned: a Final Reviewer has "returned" a report to a Reviewer for further analysis. • Complete: the Reviewers have approved the report.
Status	The review status signifies the current state of the report along with the state of the review process. • On time: The report review is on-time regarding the due date. • Approaching due date: The review due date is approaching and the review process has not yet been completed. The default time allowed before a review is given a yellow status is 80% of the elapsed time between the Creation date and the Due date. This threshold can be changed in *General Settings*. • Past due date: The report review is over the due date.
Rating	This attribute of a report review activity is specified by the reviewer. The four states are: • No rating (no impact) • Low (minimal impact) • Medium (some impact) • High (High impact = High Risk)

By default, some columns are hidden to show more important information. To view the hidden columns, click the down-arrow in a column header and select the additional columns you want to view.

Report Tab

The **Report** tab displays the results of a report selected in the **Reports for Review** panel. Its header shows the Report Name, the query time range (From - To), the source appliance from which the report was retrieved, and the retrieval status of the report.

Report tab



Report tab decsription

Element	Description
Report Query Time Range	The Query Time range corresponds to the time on the appliance where the report was retrieved. Report queries always use a query time range starting at 12am. This will include all results for the day/week/month depending on the frequency selected.
Report Source Appliance	A link on the Report tab, **Source Appliance**, is provided to easily navigate to the appliance where the report results were retrieved. This allows you to investigate any anomalies found in the Report Results.
Report Query Status	The Report Query Status, if any, is located below the Query Time Range. • If the Report query returned no results for the specified Query Time Range, then **No data available for specified report query** will be displayed. • If the report query exceeded the maximum result limit, then **Report result count exceeded max limit** will be displayed.

Review History and Comments Tab

All events associated with a compliance report that is scheduled and assigned for review are recorded to meet the compliance activity documentation requirements of an audit. You can review the life cycle of a compliance report from the time of creation to completion in the **Review History and Comments** tab

Events are recorded and time-stamped when:

- the report results are retrieved from the Appliance and the review task is created,
- anytime the report state is changed by a Reviewer or Administrator (for example, when the report is Claimed, Returned, or Approved),
- or when comments are added by a Reviewer or Administrator (note that they can be edited/deleted by clicking on the [Edit]/[Delete] hyperlinks in the **Description** column).

Tips About Columns in the Manage Review Tables

- To sort a column by ascending or descending order, click once on its column header. Sorted columns have a dark grey header and their names are followed either by an upward (ascending) or a downward (descending) arrow.
- To rearrange the order/position of columns, drag-and-drop column headers on the column header row.
- To select the columns that you want to display, click the down triangle arrow on the right hand side of any column header, select the **Columns** menu and tick their corresponding check boxes.
- To resize columns to the desired width, mouseover their column dividers and click-and-drag the left/right arrow.

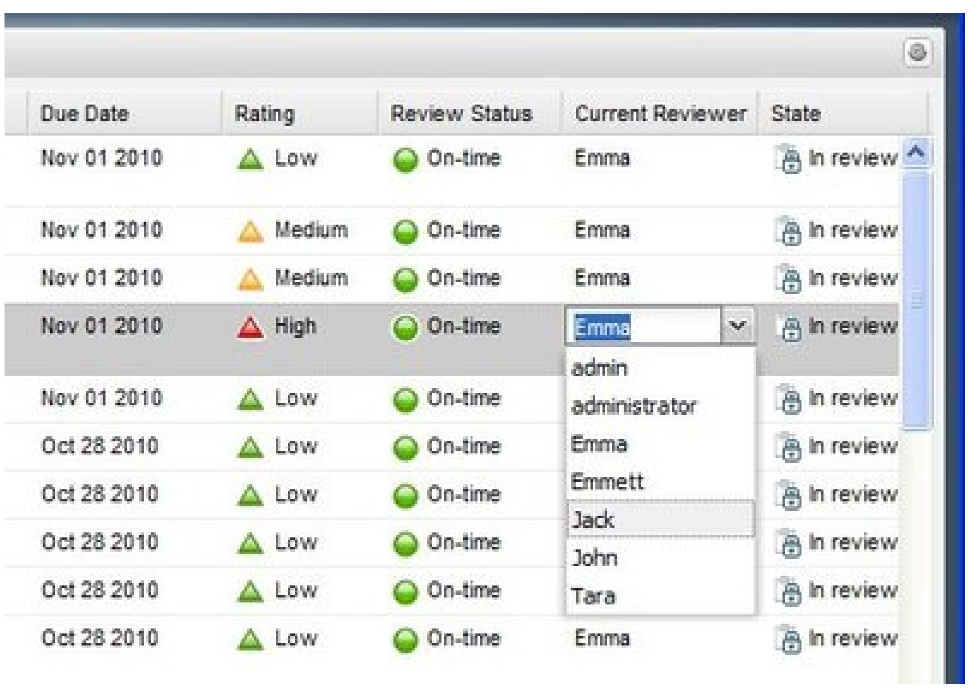
Reassigning a Report to Another Reviewer

Procedure

1. From the **Reports for Review** panel, select a report to reassign by double-clicking in the **Current Reviewer** column.

   A combo box listing the possible reviewers appears.

   Selection of Reviewer from the Current Reviewer Column

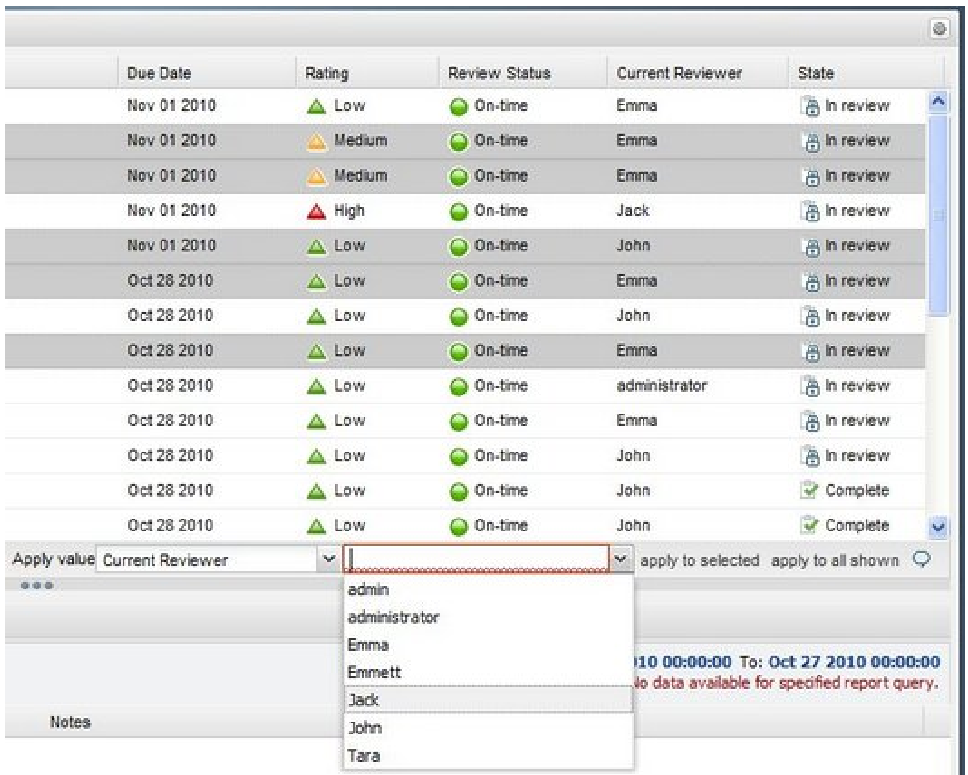
   

2. From the combo box, select a new reviewer.
3. Press **Enter** or click anywhere else on the panel.

   OR

1. Select one or more reports that need a Reviewer change.
2. Go to **Apply Value** at the bottom of the panel, and from the first drop-down list, select **Current Reviewer**.
3. From the second drop-down list, select the reviewer's name.

   Selection of Reviewer from the bottom Toolbar



4. Click **apply to selected**. The selected reviewer is applied to the selected reports.

   You can also click **apply to all** shown if you want to apply a new value to all the reports displayed on the current page.

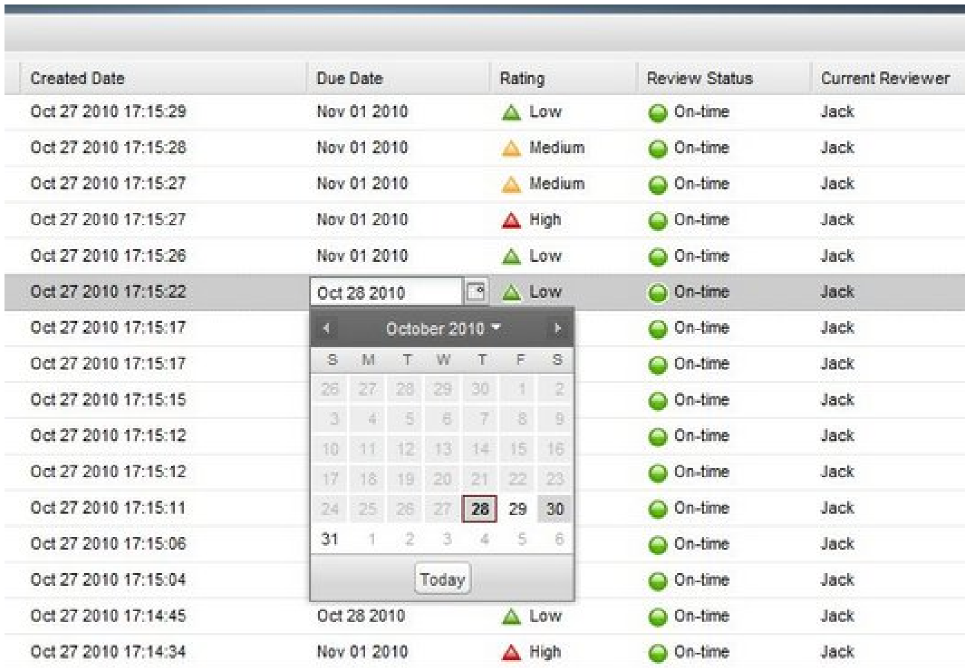
Changing the Review Due Date

Procedure

1. From the **Reports for Review** panel, select a date to change by double-clicking in the **Due Date** column.

   The cell is highlighted and displays a calendar icon on its right.
2. Click the calendar icon to select a new due date

Selection of Date from the Due Date Column



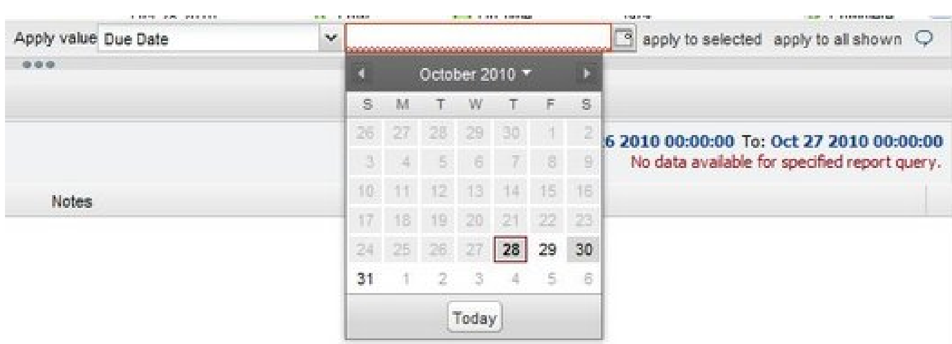
3. Press **Enter** or click anywhere else on the grid.

   The new due date is assigned to this report.

   OR

1. Select one or more review Due Dates to change.
2. Go to **Apply Value** at the bottom of the panel, and from the first drop-down list, select **Due Date**.
3. From the second drop-down list, select the due date from the calendar

   Selection of Due Date from the bottom Toolbar



4. Click **apply to selected**. The selected Due Date is applied to the selected reports.

You can also click **apply to all shown** if you want to apply a new value to all the reports displayed on the current page.

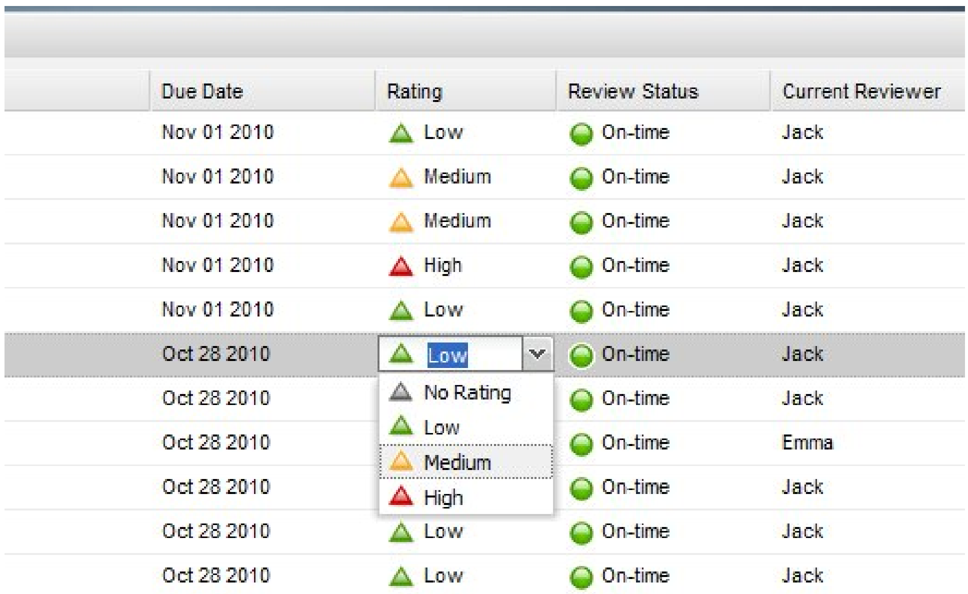
Changing the Review Rating

Reviewers can use Low, Medium, High or No Rating rating levels to prioritize investigations and follow-up activities as part of the compliance review process.

Procedure

1. From the **Reports for Review** panel, select a rating to change by double-clicking in the **Rating** column.
   The cell turns into a drop-down list.
2. From the drop-down list, select a new rating.

   Selection of Rating from the Rating Column



	Due Date	Rating	Review Status	Current Reviewer
	Nov 01 2010	Low	On-time	Jack
	Nov 01 2010	Medium	On-time	Jack
	Nov 01 2010	Medium	On-time	Jack
	Nov 01 2010	High	On-time	Jack
	Nov 01 2010	Low	On-time	Jack
	Oct 28 2010	Low	On-time	Jack
	Oct 28 2010	No Rating	On-time	Jack
	Oct 28 2010	Low	On-time	Emma
	Oct 28 2010	Medium	On-time	Jack
	Oct 28 2010	High		
	Oct 28 2010	Low	On-time	Jack
	Oct 28 2010	Low	On-time	Jack

3. Press **Enter**.

   The new rating is assigned to this report.

   OR

   1. Select one or more ratings to change.
   2. Go to **Apply Value** and from the first drop-down list, select **Rating**.
   3. From the second drop-down list, select a specific rating

   Selection of Rating from the bottom Toolbar

4. Click **apply to selected**. The Rating is applied to the selected reports.

   You can also click **apply to all shown** if you want to apply a new value to all the reports displayed on the current page.

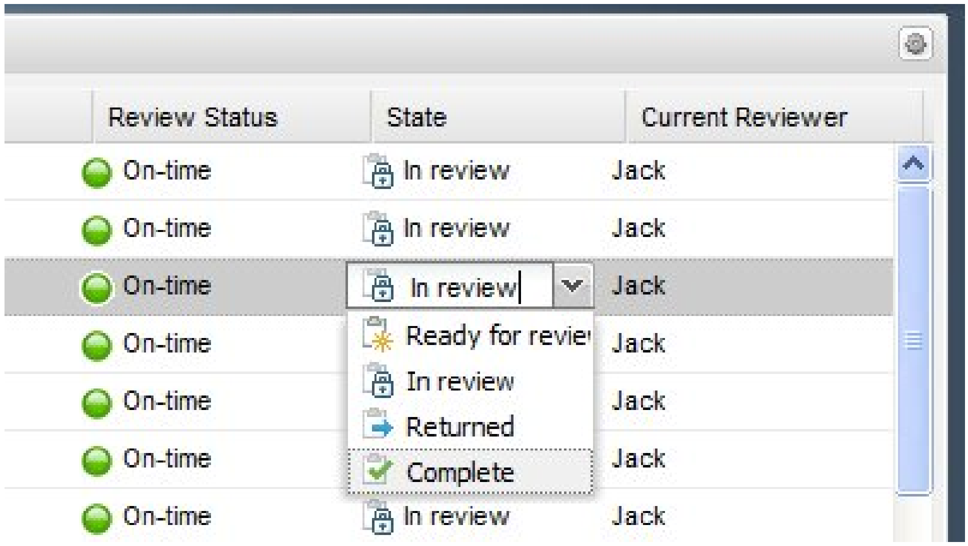
Changing the Review State

Procedure

1. From the **Reports for Review** panel, select a state to change by double-clicking in the **State** column.
   The cell turns into a drop-down list.

2. From the drop-down list, select a new state, i.e., Ready for Review, In Review, Returned, Complete

   Selection of State from the State Column

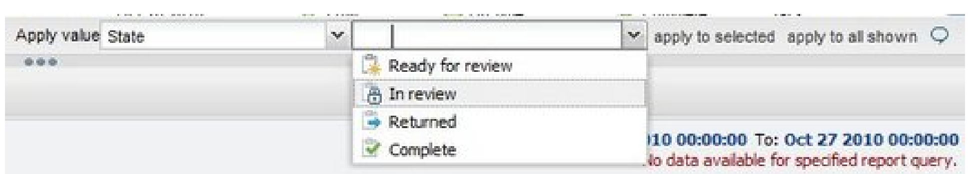


3. Press **Enter** or click anywhere else on the grid. The new state is assigned to this report.

   OR

   1. Go to **Apply Value** at the bottom of the panel, and from the first drop-down list, select **State**.
   2. From the second drop-down list, select the specific state: Ready for Review, In Review, Returned, Complete

      Selection of State from the bottom Toolbar



   3. Click **apply to selected**. The State is applied to the selected reports.

You can also click **apply to all shown** if you want to apply a new value to all the reports displayed on the current page.

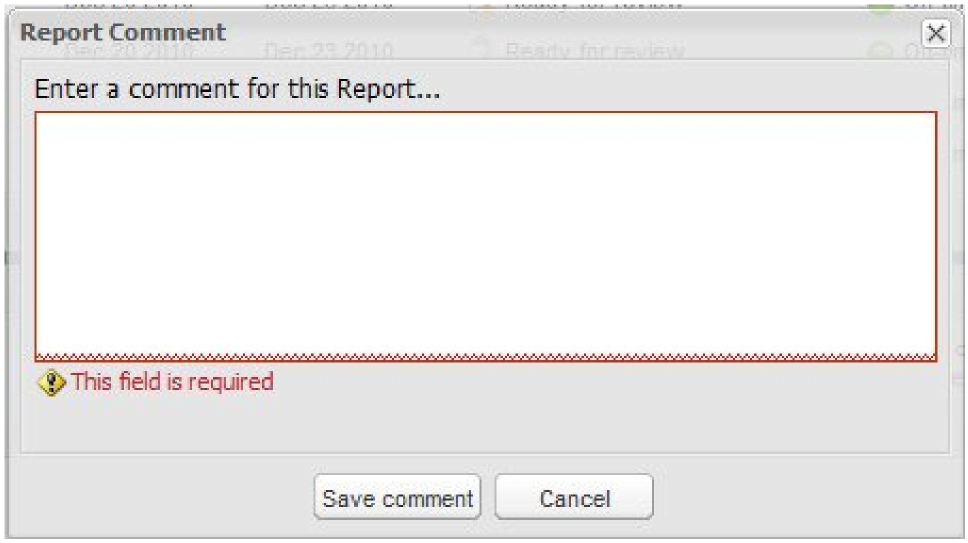
Adding a Comment to a Report

An administrator can add comments to the review. For example, an administrator can provide a summary of the impact, corrective actions, and/or steps for investigation relevant to the report.

Procedure

1. Click the **Comment** button at the bottom right hand corner of the panel. The **Report Comment** dialog box opens.
2. Enter a comment text in the **Report Comment** dialog box.

Report Comment Dialog Box



3. Click **Save comment**.

   Your comment is saved and added to the list of the **Review History & Comments** tab.

   Comment Listed in the Review History & Comments Tab

A comment can be edited or deleted by clicking the [Edit]/[Delete] link in the **Description** column.

Filtering and Sorting Reports

Procedure

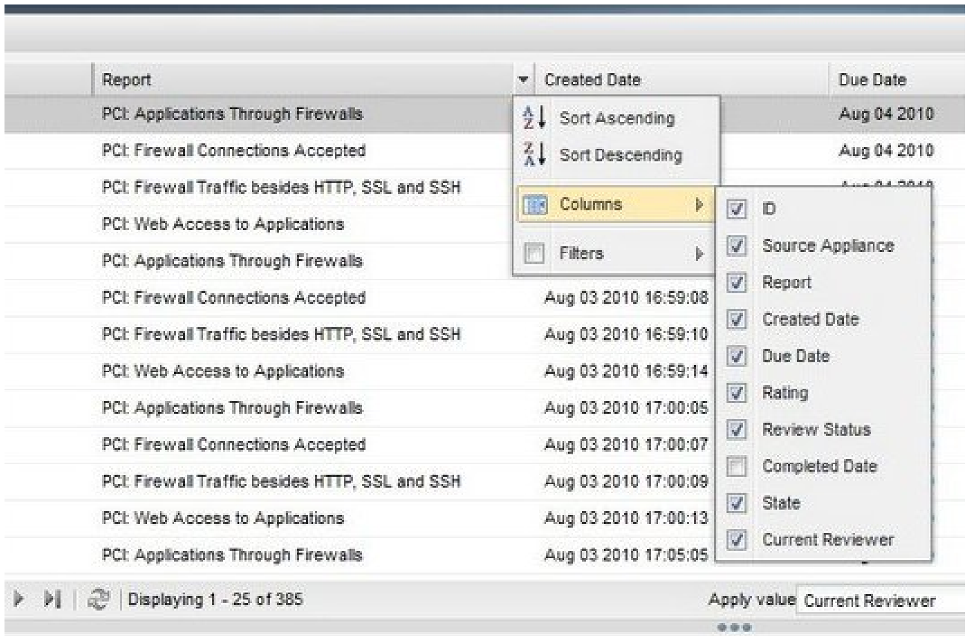
1. Click once on any column to change the sort order.

   To keep satisfying perfomances avoid sorting the columns: Current Reviewer, Report and Source Appliance.

2. To filter the view, mouseover the column header row and select the down triangle arrow to display the various applicable filters.

   A drop-down list will appear, providing the following selections: Sort Ascending, Sort Descending, Columns (ID, Source Appliance, Report, Created Date, Modified, Completed Date, Current Reviewer, Due Date, State, Review Status and Rating), and Filters

Reports for Review Filtering and Sorting Options



To remove all the filters applied to the Reports for Review table click the clear all filter conditions button .

Monitoring Report Results

The **Report** tab contains a table displaying the results of the report selected above, in the **Reports for Review** panel. These report results can be considered as summary views of similar report rows. You will moreover see that many reports display a **Count** column to indicate precisely the number of rows corresponding to each report result. The count hyperlink allows to drill-down to the report rows, that is to say to the **Report Result Details** level.

Contents

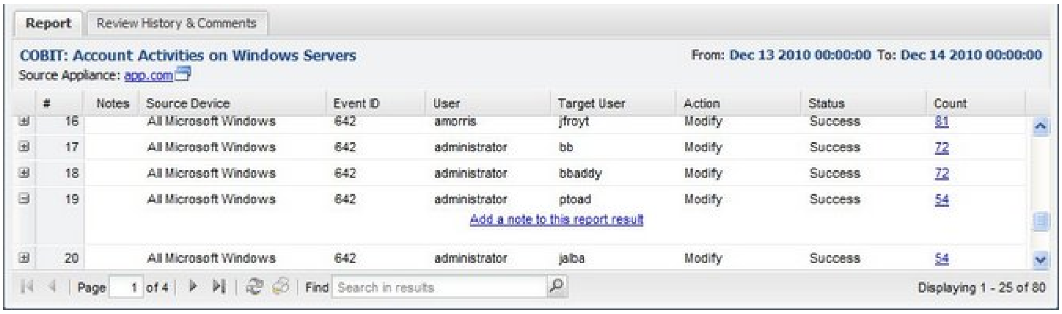
Adding/Viewing Report Result Annotations

Each result in a report can contain one or multiple annotations, or notes. You can do a fine-grain commenting of the report, down to the report result level. Report result annotations are archived and can be edited or deleted once created.

Procedure

1. Select a Report in the **Reports for Review** list.
2. Double-click a report result in the **Report** tab to expand it.

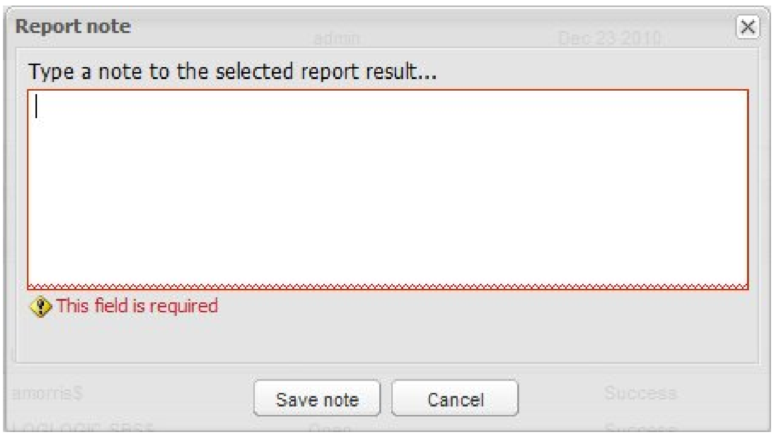
Add a Note to this Report Result Link



3. Click the **Add a note to this report result** link.

   The **Report note** dialog box opens.

   Report note Dialog Box

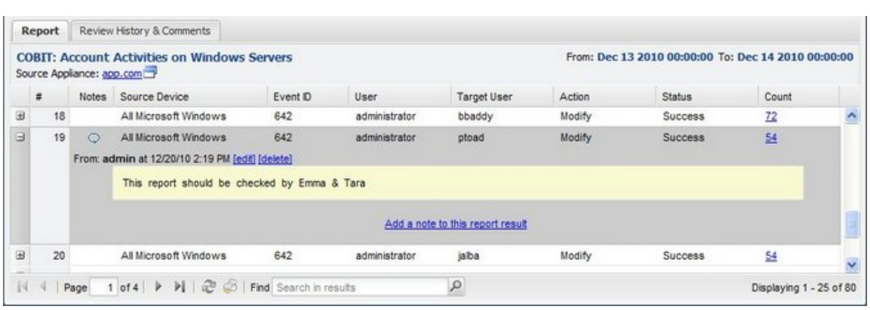


4. Type in your comment and click **Save note**.

   The Annotation is displayed below the report result with the timestamp of when the Annotation was created, and the User Account that created the Annotation.

   The report results that have an annotation, display an icon in the **Notes** column. Double-click the report result to display all its annotations.

   Display of Report Result Annotation



The report result note can be edited or deleted by clicking the [Edit]/[Delete] links.

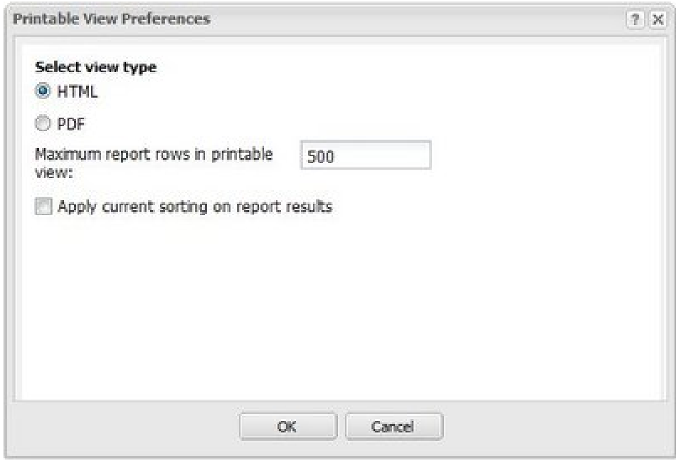
Printing Report Results

Procedure

1. Click the **printer** icon located at the bottom of **Report** tab.

   The **Printable View Preferences** window opens.

Report Results Printable View Preferences



2. In the **Printable View Preferences** window, set the Print settings as needed.

Printable View Preferences

Setting	Description
HTML/PDF	Use these radio buttons to select the file format for the printable view, i.e., either **HTML** or **PDF**
Maximum report rows in printable view	Enter the maximum number of report rows that must be displayed in the printable view.
Apply current sorting on reports	Tick this check box if you want your report to reflect your sorting preferences.

3. Click **OK**.

The report review is generated in the format you selected, i.e. HTML or PDF, suitable for sending to a printer or downloading for reviewing offline. The HTML and PDF versions contain the following information:

- Report Name
- Retrieval Time
- Due Date
- Name of the Current Reviewer
- Source Appliance for the Report
- Description of the report
- List of controls the report addresses
- List of Report History and Comment Events
- Report Results including annotations

Drilling-Down to the Report Result Details Level

For the reports displaying a **Count** column, it is possible to drill-down to the **Report Result Details** level and see all the rows corresponding to each report result.

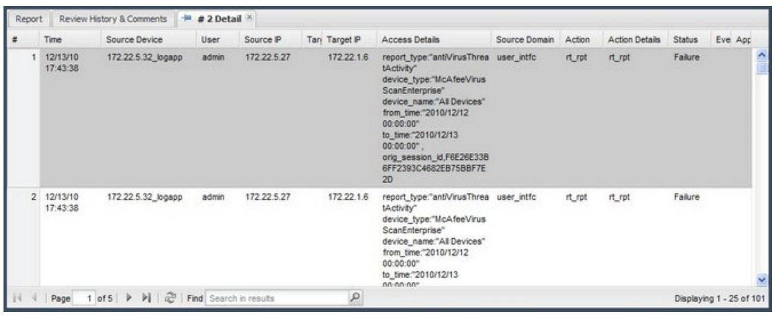
Drill-down actions depend on the appliance load and might therefore be very long (and sometimes fall in timeout). Obviously, the more powerful the hardware the faster the performances.

Procedure

1. In the **Count** column of the **Report** tab, click the hyperlink of a report result.

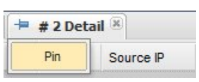
   A new tab appears in the bottom panel. Its label displays the line number of the report result (the format is # **<line number> Detail**) as shown in the **Report** tab. The generation of the report result details can take a few minutes.

   Report Result Details Tab

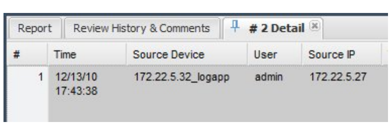
2. To save the report result detail tab for future use, mouseover the tab label and click **Pin** in the pop-up menu

   Report Result Detail Tab Pin Option

   Once pinned, the report result detail tab will always be displayed in the bottom panel of the Review dashboard when you select the same report in the **Reports for Review** panel

   Pinned Report Result Detail Tab

3. You can repeat the three first steps to open and pin more report result detail tabs.

   If you want to unpin a tab, mouseover its tab label and click **Unpin** in the the pop-up menu.

   All data of drill-down actions will be deleted from the CM database every 24 hours unless report result detail tabs are pinned.

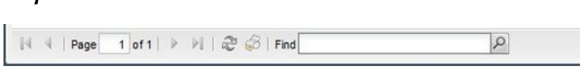
Searching in the Report tab

Use the **Find** box at the bottom of the panel to quickly filter the report results.

Procedure

1. Enter text into the **Find** box

   Report tab Find Box

2. Press **Enter**.

   The view will be filtered to display only the results containing the matching text (this text highlighted in bold characters).

Consulting the Review History & Comments

To view the change history and comment of a report review listed in the **Review Dashboard**, select it and consult the list displayed in the **Review History & Comments** tab.

Administration

The Administration menu allows you to manage the following CM settings:

- User Accounts
- Logs generated for each event/action performed in the application
- General Settings:
  - Report query and review settings
  - Retention policies
  - Password expiration security policy
  - SMTP server settings used for sending notifications to Reviewers and Executives
  - Syslog log forwarding
  - Customized logo for the menu bar and display of Consent Banner on user login
- Backup/Restore operations
- Add, configure, and remove the LX/ST/MX appliances from which report definitions will be retrieved
- Remote Authentication server settings for Radius or Active Directory servers

The Administration menu is available only to user accounts with Administrator role.

Contents

User Management

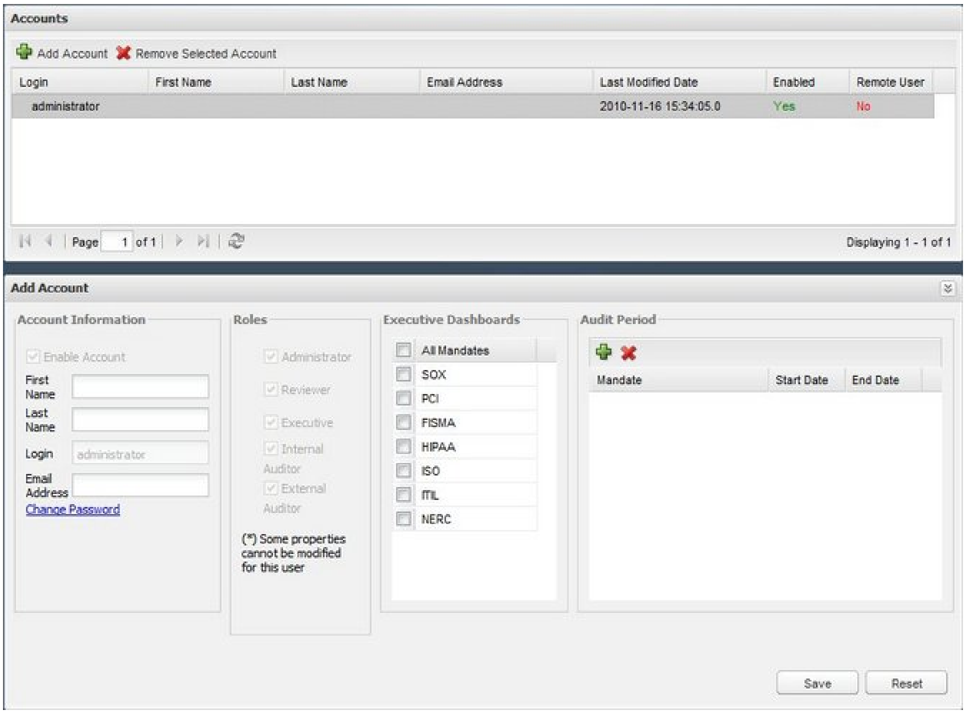
In **Administration** > **User Management**, the CM administrator can add, edit and delete LogLogic® Compliance Manager user accounts.

Contents

Description of the User Management View

The User Management view displays two panels, i.e., Accounts and Add/Edit Account

User Management View

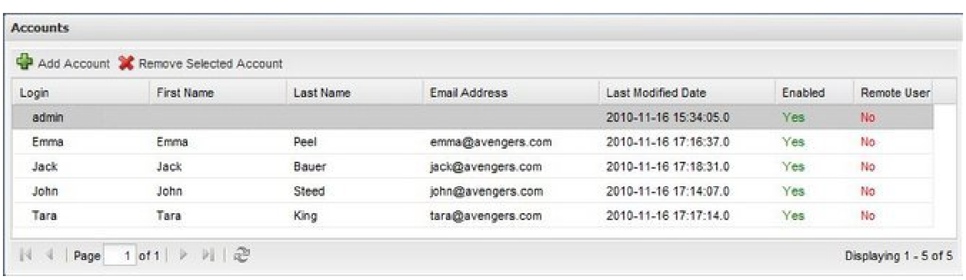


Accounts Panel

The top panel, **Accounts**, provides a list of all user accounts, their statuses (enabled/ disabled) and whether they are managed locally or remotely.

When a user account is selected in the **Accounts** panel, its associated roles, Dashboards (for Executive role), and allowed audit periods (for Internal and External Auditor roles) are displayed below, in the **Edit Account** panel.

Accounts Panel



Accounts Panel Description

Icon	**Description**
	Opens the **Add Account** panel which allows to define a new user account.
	Allows to delete a selected user account. **Note:** The administrator account cannot be deleted.
Column	**Description**

Login	Indicates the login of the user account
First Name	Indicates the user's first name
Last name	Indicates the user's last name
Email Address	Indicates the user's email address
Last Modified Date	Indicates the date of the user account's last modification
Enabled	Indicates whether the user account is currently enabled or disabled in CM
Remote User	Indicates whether the user account is managed locally or remotely (No/ Yes).

Column Tips

- To sort a column by ascending or descending order, click once on its column header. Sorted columns have a dark grey header and their names are followed either by an upward (ascending) or a downward (descending) arrow.
- To rearrange the order/position of columns, drag-and-drop column headers on the column header row.
- To select the columns that you want to display, click the down triangle arrow on the right hand side of any column header, select the **Columns** menu and tick their corresponding check boxes.
- To resize columns to the desired width, mouseover their column dividers and click-and-drag the left/right arrow.

Add/Edit Account Panel

The bottom panel, **Add/Edit Account**, allows to define the user account's properties and its role(s).

Add/Edit Account Panel Description

Setting	Title	Description
Account Information	Enable Account	Tick this check box to enable the user account in CM
	First Name	Enter the user's first name
	Last Name	Enter the user's last name
	Login	Enter the login of the user account
	Email Address	Enter the user's email address
	Password/Confirm Password	Enter the user's password
Roles	See User roles table.Table 37	
Executive Dashboards		

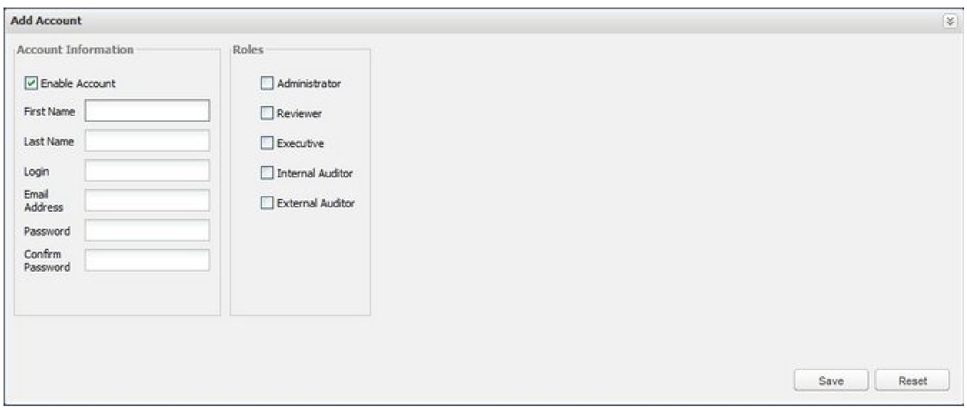
Setting	Title	Description
Audit Period		

Adding a User Account

Procedure

1. Select **Administration** > **User Management** from the navigation menu.
2. In the **Accounts** panel, click **Add Account**. The **Add Account** panel appears at the bottom of the screen.

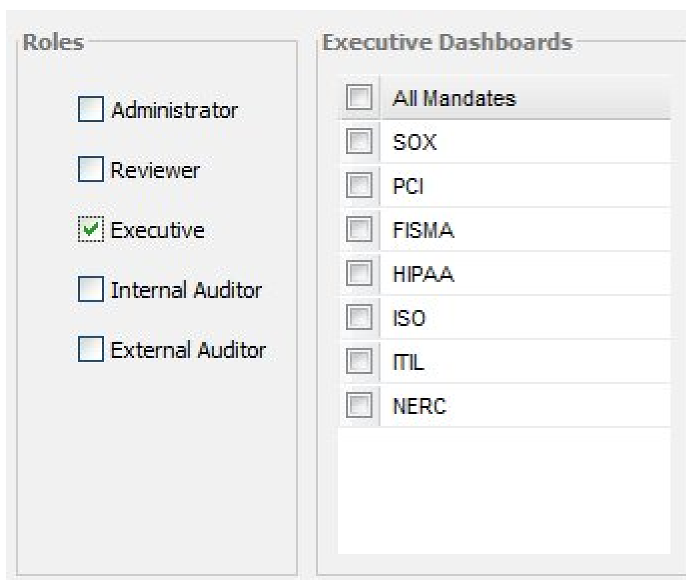
   Add account panel

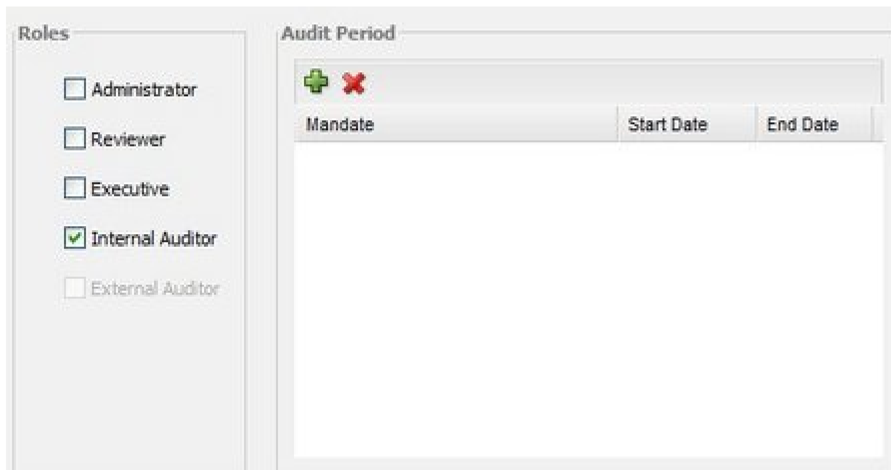
3. In the **Add Account** panel, enter the following account information: First name, Last name, Email address (the email address is used to send notifications), Login, Password, Confirm Password.
4. Click the **Enable Account** check box. By deselecting this check box, a user account can be disabled without being deleted.
5. Under **Roles**, assign one or more roles for this user account.

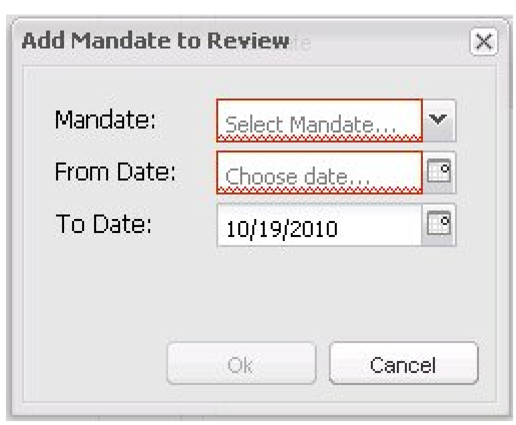
   User Roles

Role	Description
Administrator	The Administrator can: • Enable the compliance review process by scheduling reports and specifying reviewers for the report results • Manage users and roles • Review LogLogic® Compliance Manager application history • Configure system wide settings for the LogLogic® Compliance Manager appliance • Manage the mandates and controls by creating custom ones and enabling the mandates or the controls relevant for the organization compliance scope. In LogLogic® Compliance Manager, the work areas of Administrators are the Review Management and the Administration menus.

<table>
<tr><th>Role</th><th>Description</th></tr>
<tr><td>Reviewer</td><td>
A user with this role performs detailed research and analysis. Reviewers are required to periodically (daily or on an alternate regular schedule) review reports. They are also delegated the investigation tasks and are responsible for preparing summarized information for executives.
Reviewers provide the critical human intelligence to identify and guide the organization compliance process.
In LogLogic® Compliance Manager, the work area of Reviewers is the Review Dashboard.
</td></tr>
<tr><td>Executive</td><td>
A user with this role has an at-a-glance view of the timeliness of the compliance activities and ratings which includes the assessment by the compliance team.
In LogLogic® Compliance Manager, the work area of Executives is the Executive Dashboard.
When this check box is ticked, an Executive Dashboards pane appears on the GUI to let you select the mandates that will be available for the user in the Dashboard > Executive view.


</td></tr>
</table>

<table>
<tr><th>Role</th><th>Description</th></tr>
<tr><td>Internal Auditor</td><td>
A user with this role both validates the compliance to mandates and checks that the LogLogic® Compliance Manager review process is correctly applied by the various CM users. The Internal Auditor’s role is to prepare the organization to a compliance audit made by an External Auditor. Internal Auditor can write comments to point out specific things to the compliance Reviewers.
In LogLogic® Compliance Manager, the work area of Internal Auditors is the Audit Dashboard where they can add annotations.
When this check box is ticked, an Audit Period pane appears on the GUI to let you define the mandates that will be available for the user in the Dashboard > Audit view, and the period that will be covered by the audit.


Click the Add new mandate review period button 
The Add Mandate to Review dialog box opens to let you select a mandate as well as the start and end dates of the Audit review.


Click OK.
The mandate audit period is added to the Audit Period table.
</td></tr>
</table>

Role	Description
External Auditor	A user with this role both validates the compliance to mandates and checks that the LogLogic® Compliance Manager review process is correctly applied by the various CM users of an organization. Contrary to Internal Auditors, External Auditors cannot add annotations. In LogLogic® Compliance Manager, the work area of External Auditors is the *Audit Dashboard*. **Note:** See the Internal Auditor description above to see how to add Audit Periods.

6. Click **Save**. The new user has been added to the system. Otherwise, to revert your entries, click **Reset**.

Login names are unique and cannot be changed.

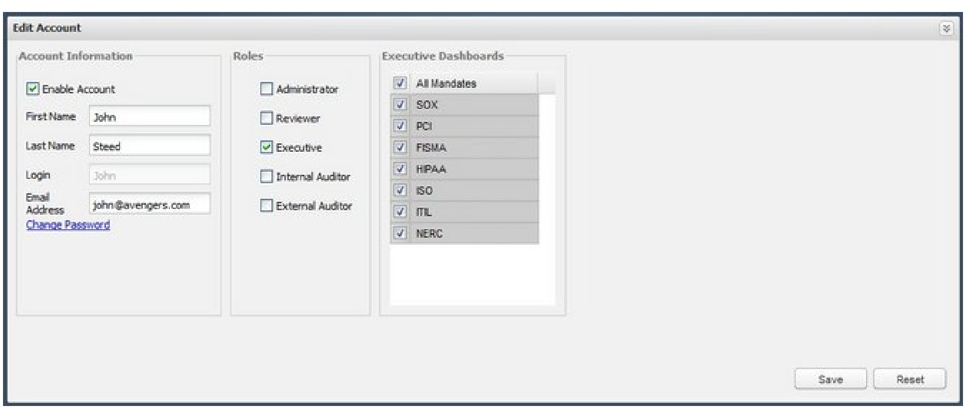
Editing a User Account

To edit a user account:

Procedure

1. Select **Administration** > **User Management** from the navigation menu.
2. In the Accounts panel, select a user account.
The account information appears in the Edit Account panel. (see Figure 105)

Figure 105 Edit Account Panel



3. In the **Account Information** pane:
a) Either deselect the Enable Account checkbox or keep it enabled
b) Edit the following properties: First name, Last name, Email address, Password.
4. Under Roles, define the user account's profile by associating it to roles: Administrator, Reviewer, Executive, Internal Auditor, External Auditor. See Adding a User Account for a detailed description of each role.

Roles for user accounts managed by a remote authentication server (i.e., Radius or Active Directory) must be edited on that server. See Remote Authentication

5. Click **Save**. The new information has been updated. Otherwise, to revert your entries, click **Reset**.

You cannot change the role of the default administrator account nor deselect Enable

Account. Once a login name is created, it cannot be changed. If the user account has the Reviewer

role, and it is being disabled, or if a Reviewer role is being removed, you must identify an alternate

reviewer for any reports potentially assigned to the user account being edited. To complete the

process, click Reassign (see Figure 107)

Changing a User Account Password

The passwords of user accounts managed by a Remote Authentication Server (i.e., Radius or Active Directory) must be set on the Remote Authentication server itself (see Remote Authentication). Therefore, the following procedure does not apply to these user accounts' passwords.

Procedure

1. Select **Administration** > **User Management** from the navigation menu.
2. In the **Accounts** panel, select a user account.
   The account information appears in the **Add Account** panel.
3. In the **Account Information** settings, click the **Change Password** link.
4. Enter the new Password in the text box and confirm the password in the **Confirm Password** text box.

   Change password settings

5. Click **Save**.
6. To cancel this change, click the **Cancel Changing** link.
   After a password has been reset, the user will be prompted to change their password upon login.

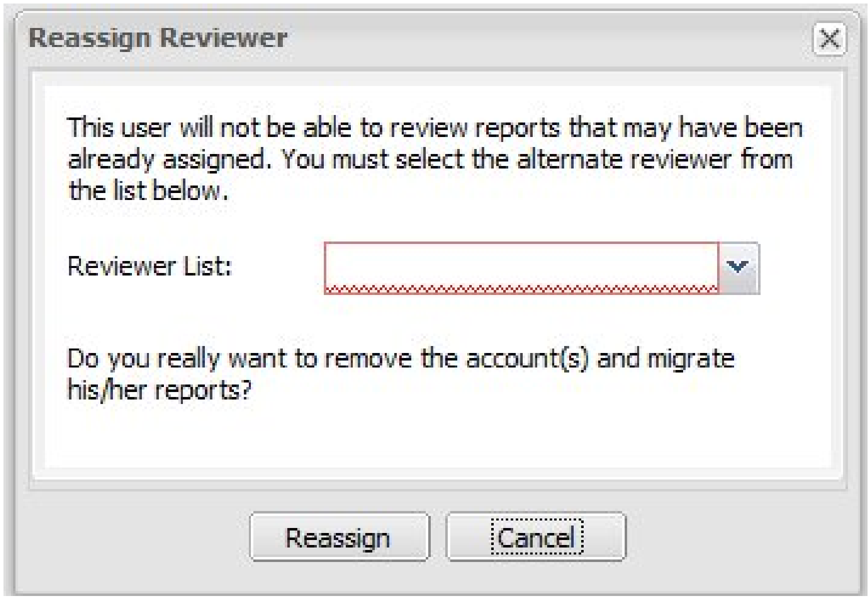
Deleting a User Account

Procedure

1. Select **Administration** > **User Management** from the navigation menu.
2. In the **Accounts** panel, select one or more user accounts.
3. Click **Remove Selected Account**.

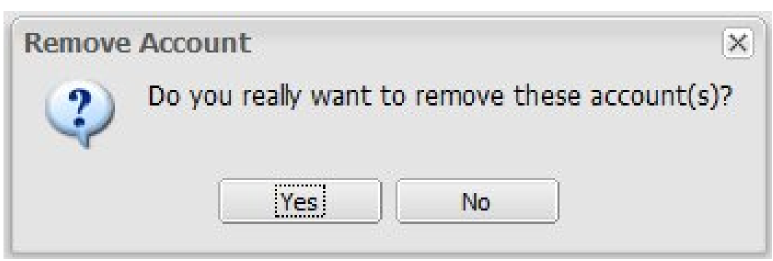
4. If the user account has the Reviewer role, the **Reassign Reviewer** dialog box opens to let you identify an alternate reviewer for any reports potentially assigned to the removed user account (see Figure 107). To complete the process and remove the user account, click **Reassign**.

   Reassign Reviewer Dialog Box

   If the user account does not have a Reviewer role, a **Remove Account** dialog box is displayed asking if you want to delete this account. Click **Yes** to remove the account.

   Remove Account Dialog Box

   The account has been removed from LogLogic® Compliance Manager.

Sorting User Accounts

To filter or sort user accounts, mouseover the column header row and select the down triangle arrow to display the various applicable filters.

A drop-down list will appear, providing the following selections: Sort Ascending, Sort Descending, Columns (Login, First Name, Last Name, Email Address, Last Modified Date, Enabled, and Remote User).

Application Event Log

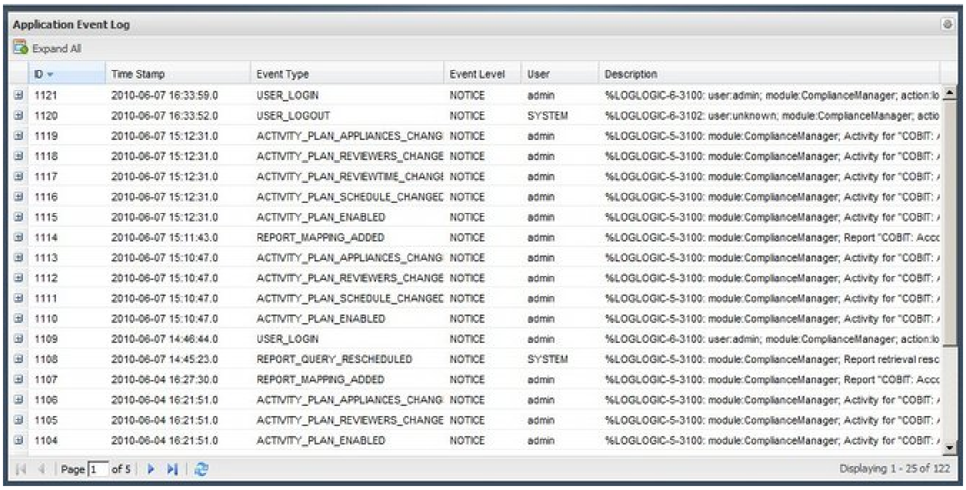
In **Administration** > **Application Event Log**, the CM administrator can view LogLogic® Compliance Manager informational, warning, and error log messages.

Contents:

Description of the Application Event Log View

The **Application Event Log view** displays all the system and user activities that have been captured as an audit trail of the system

Application Event Log View



Application Event Log View Description

Icon	Description
	Use the Expand All button to expand all the table rows at once. The whole description of each row is thus displayed. Use the Collapse All button to collapse all the table rows at once.
Column	**Description**
ID	Indicates the ID of the event log
Time Stamp	Indicates the time stamp of the event log. The time format is YYYY-MM-DD hh:mm:ss.

Event Type	Indicates the event type: • UNKNOWN • REPORT_QUERY_START • REPORT_QUERY_FINISH • REPORT_QUERY_TASK_CREATED • REPORT_QUERY_EXCEPTION • REPORT_QUERY_ERROR • REPORT_QUERY_COMPLETED • REPORT_WRITE_ERROR • EMAIL_SERVER_INVALID • EMAIL_FROM_ADDR_INVALID • EMAIL_TO_ADDR_INVALID • EMAIL_PREP_ERROR • EMAIL_SEND_ERROR • APP_SETTINGS_UPDATED • APPLIANCE_CREATED • APPLIANCE_UPDATED • APPLIANCE_REPORT_RETRIEVAL • APPLIANCE_DELETED • AUTH_SERVER_CREATED • AUTH_SERVER_UPDATED • AUTH_SERVER_DELETED • NETWORK_INTERFACES_UPDATED • USER_CREATED • USER_UPDATED • USER_DELETED • USER_ROLES_UPDATED • USER_PASSWORD_EXPIRED • USER_PASSWORD_CHANGED • USER_TASKS_REASSIGNED • ACTIVITY_PLAN_ENABLED • ACTIVITY_PLAN_DISABLED • ACTIVITY_PLAN_SCHEDULE_CHANGED • ACTIVITY_PLAN_REVIEWTIME_CHANGED • ACTIVITY_PLAN_REVIEWERS_CHANGED • ACTIVITY_PLAN_APPLIANCES_CHANGED • DISK_SPACE_INFO • PURGED_COMPLETED_TASK

Event Type - continued	• PURGED_REVIEW_TASK • PURGED_CLOSED_TASKS • PURGED_APP_HISTORY • PURGED_TASK_REPORT_RESULTS • WORK_ITEMS_CREATED • WORK_ITEMS_RECOVERED • AUTHENTICATION_BAD_CREDENTIALS • USER_FIRST_TIME_LOGIN • USER_ACCEPT_EULA • PURGED_REPORT_TABLE • PURGED_TASK_REPORT_TABLE • AUTHENTICATION_FAILURE • LICENSE_CHECK • USER_LOGOUT • USER_LOGIN • REPORT_MAPPING_ADDED • REPORT_MAPPING_REMOVED • REPORT_MAPPING_ERROR • REPORT_MAPPING_WARNING • USER_ACCEPT_BANNER • USER_REJECT_BANNER • USER_REJECT_EULA
Event Level	Indicates the event level: • EMERG • ALERT • CRIT • ERR • WARNING • NOTICE • INFO • DEBUG
User	Indicates the event creator: • SYSTEM: For events related to LogLogic® Compliance Manager "background activities" such as Report Queries, Report Retention, and email notifications. • <USER name>: For event performed by users (the user name is indicated in the column)

Description	Indicates the Syslog data.

Column Tips

- To sort a column by ascending or descending order, click once on its column header. Sorted columns have a dark grey header and their names are followed either by an upward (ascending) or a downward (descending) arrow.
- To rearrange the order/position of columns, drag-and-drop column headers on the column header row.
- To select the columns that you want to display, click the down triangle arrow on the right hand side of any column header, select the **Columns** menu and tick their corresponding checkboxes.
- To resize columns to the desired width, mouseover their column dividers and click-and-drag the left/right arrow.

Viewing LogLogic® Compliance Manager Events

To view LogLogic® Compliance Manager events, select **Administration** > **Application Event Log**.

The **Application Event Log** view is displayed. This includes all the system and user activities that have been captured as an audit trail of the system. These logs can be forwarded to another LogLogic LX appliance.

To view the entire description (i.e., Syslog data) of an event log, click the plus [+] button on the left of its row. The row will expand to display the entire description. You can also use the **Expand All** button to expland all rows.

The user will be "SYSTEM" for any messages related to LogLogic® Compliance Manager "background activities" such as Report Queries, Report Retention, and email notifications.

Filtering and Sorting Logs

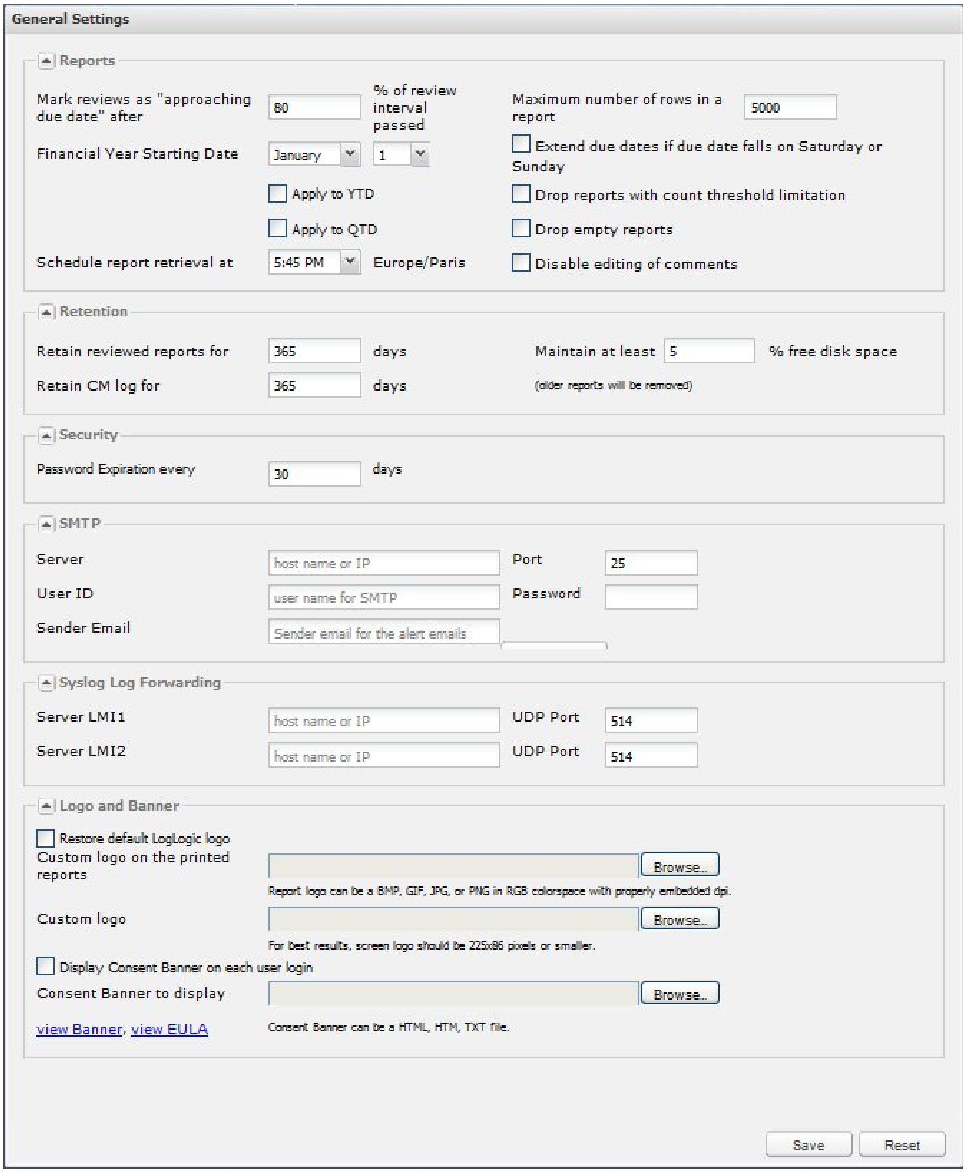
To filter or sort logs, mouseover the column header row and select the down triangle arrow to display the various applicable filters.

A drop-down list will appear, providing the following selections: Sort Ascending, Sort Descending, Columns (ID, Time Stamp, Event Type, Event Level, User, and Description), and Filters.

To remove all the filters applied to the Application Event Log table click the clear all filter conditions button .

General Settings

In **Administration** > **General Settings**, the CM administrator can configure general system settings related to scheduled reports, report retention, password expiration, logos and banners, SMTP server configuration and Syslog log forwarding.



General Settings

Setting	Entry	Description
Reports	Maximum number of rows in a report	Set the limit of rows to view in each report. The maximum is 5000.
	Mark reviews "as approaching due date" after [n]% of review interval passed	Enter a percentage. This percentage is used to calculate the timeliness status of any Report Reviews.

Setting	Entry	Description
	Financial Year Starting Date	Set the fiscal/financial year starting date. CM will take into account this custom starting date instead of the default calendar year starting date (i.e. January 1st) in all Dashboards. You can choose whether the customized financial year starting date shall impact the Quarter to Date (QTD) and Year to Date (YTD) predefined periods. Note that it cannot impact the Month to Date (MTD) predefined period. For example, if the custom fiscal year starting date is set to March 13th and applied to YTD, this date will be used as the year starting date in all CM Dashboards. If it is applied to QTD, then Quarter 1 will begin on March 13th and the following Quarters will be shifted accordingly.
	Extend due dates if due date falls on Saturday or Sunday	Select this check box to enable this feature.
	Schedule report retrieval at	Select the time of day to start the daily report retrieval job. This is a background task that queries appliances based on the Report Schedules. Typically, this time should be set to some time after midnight so that daily reports are retrieved from the previous day, and ready to review the following day.
	Drop reports with count threshold limitation	Drops reports if their counts are below the threshold specified for the **Drop reports with less than <n> counts** option in Review Management > Schedule Report.
	Drop empty reports	Drops reports which have no report results (empty reports).
	Disable editing of comments	Tick this check box if you want to disable the edition of comments.
Retention	Retain reviewed reports for [n] days	Select the number of days during which reports will be retained in the CM database. Note that all associated report details will also be deleted when this retention period is crossed.

Setting	Entry	Description
	Maintain at least [n]% free disk space	This is the threshold where the LogLogic® Compliance Manager begins to purge data. The oldest reports will be purged, regardless of the specified retention policy. Typically, this should be set to a small number such as 5%. The cleaning process respects the following order: 1 - oldest report details are removed 2 - oldest reports are removed 3 - report details are removed 4 - reports are removed
	Retain Compliance Manager log for [n] days	This is the threshold where the LogLogic® Compliance Manager begins to purge the LogLogic® Compliance Manager Application History Log. The oldest logs will be purged.
Security	Password Expiration every [n] days	Indicates the number of days after which user passwords will expire. Users will be prompted to change their passwords when this number is reached.
SMTP	Server	Enter the host name or IP address.
	Port	Enter the port number. Typically, the default port is 25 for SMTP servers. Change this value if your SMTP server uses a different port.
	User ID (Optional)	Enter the User name for this SMTP server. This value is required for SMTP servers that require authentication. Note that a specific SMTP user account might need to be created for LogLogic® Compliance Manager.
	Password	Enter the password for the User Account SMTP logon, if the User ID is required. It is mandatory in that case.
	Sender Email	Enter a valid formatted email address. LogLogic® Compliance Manager will use this address as the From address for the Executive and Reviewer notifications sent by LogLogic® Compliance Manager. Depending on your SMTP server policies, this address may or may not need to be a valid email account.
	Test Connection	Click this button to have LogLogic® Compliance Manager send a test email to verify the SMTP Settings and to ensure that the SMTP server is responding. A test email will be sent to the email address that you specified in the Sender Email field.

Setting	Entry	Description
Syslog Log Forwardin g	Server	Enter the host name or IP address of the remote server that must be used for log forwarding. CM system logs will be forwarded in UDP protocol to the remote server and will thus be analyzable by LMI appliance processes, such as security monitoring, error checking and so on. **Note:** The remote server will only receive logs. It will not be able to perform queries on CM.
	UDP Port	Enter the port number. The default port is 514. Change this value if your Syslog server uses a different port.
Logo and Banner	Restore default LogLogic logo	Select this check box to revert to the LogLogic Logo.
	Custom logo on the printed reports	Upload your company logo. This logo will appear on reports and emails.
	Custom logo	Upload your company logo to appear in the LogLogic® Compliance Manager menu bar.
	Display Consent Banner on each user login	Displays the consent banner on user each login.
	Consent Banner to display	Upload your company consent banner (HTML, HTM or txt file). It will be displayed on each user login if the **Display Consent Banner on each user login check box** is ticked.
	view Banner, view EULA	These two links allow to display the current Consent Banner and End User License Agreement (EULA).

Backup/Restore

In **AdministrationBackup/Restore**, the CM administrator can perform backup/restore operations of the CM Server database to comply with the enterprise backup policy.

The backup operation will save the following information.

Information Saved by Backup Operation

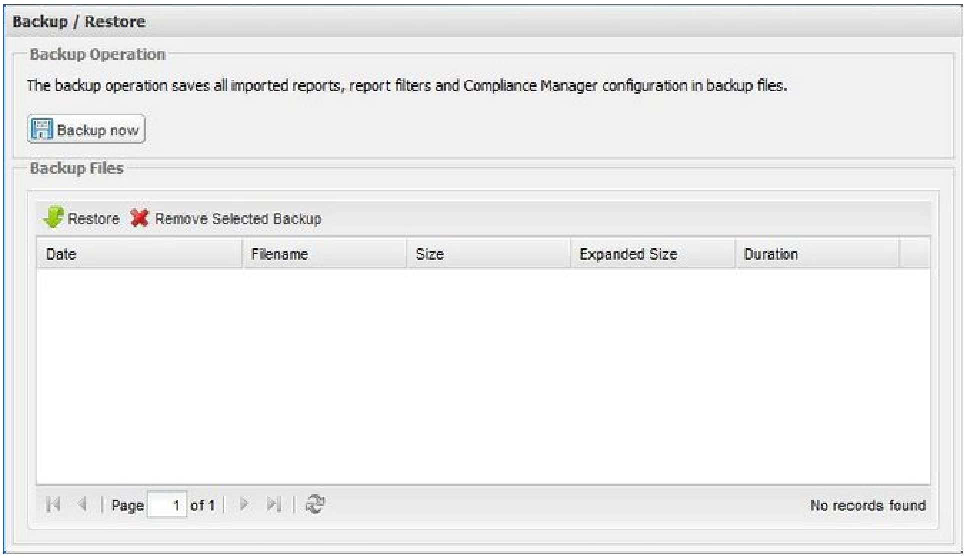
Item	Comment
User/ CM configuration	All CM configurations defined in the **Administration** menu are saved: • User accounts and their properties • General settings • Application event logs • Appliances and their configurations • Remote Authentication configuration All CM configurations defined in the **Review Management** menu are also saved: • Mandates, controls, report definitions and their respective dependencies • Scheduled report definitions • All comments and annotations added to reports, report results, mandates and controls
CM data	All CM data are saved: • All reports and report details imported from remote LMI appliances • All comments and annotations added to reports, report results, mandates and controls • All report review actions made by users (Claim, Approve, Return, Comment, Rating) • All report filters applied by reviewers (on State, Status and Rating) • All saved dashboard layouts • All CM system logs

LogLogic recommends that you backup regularly.

Contents

Description of the Backup/Restore View

The Backup/Restore view displays two panels - Backup Operation and Backup Files.



Backup Operation Panel

The top panel, **Backup Operation**, allows to launch the backup operation.

Backup Files Panel

The bottom panel, **Backup Files**, allows to restore or delete selected Backup files.

Backup Files Panel Description

Button	Description
	Click this button to restore the selected backup file.
	Click this button to delete the selected backup file.
Column	Description
Date	Displays the timestamp of the backup file. The timestamp format is YYYY-MM-DD hh:mm:ss
File Name	Indicates the name of the backup file. It is generated automatically by CM.
Size	The backup file size in MB. Unit is still MB even if the size is higher than 100 MB
Expanded Size	The backup file size in MB when unzipped.
Duration	The duration of the backup operation.

Column Tips

- To sort a column by ascending or descending order, click once on its column header. Sorted columns have a dark grey header and their names are followed either by an upward (ascending) or a downward (descending) arrow.
- To rearrange the order/position of columns, drag-and-drop column headers on the column header row.
- To select the columns that you want to display, click the down triangle arrow on the right hand side of any column header, select the **Columns** menu and tick their corresponding checkboxes.
- To resize columns to the desired width, mouseover their column dividers and click-and-drag the left/right arrow.

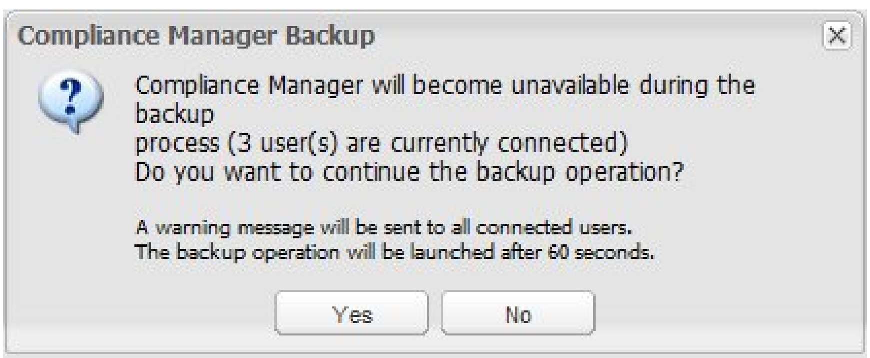
Performing a Backup

Procedure

1. Click the **Backup now** button.

   A **Compliance Manager Backup** dialog box opens, warning you that CM will be unavailable during the backup process and that connected users will have 60 seconds to save their work and log out

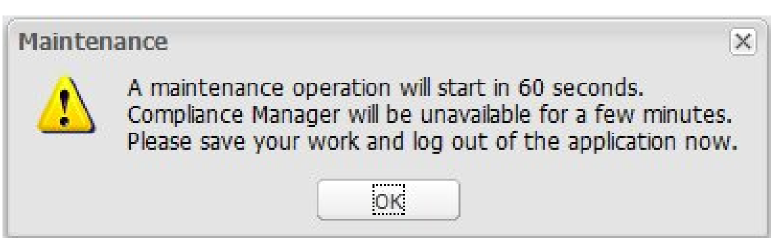
   Compliance Manager Backup Dialog Box

2. Click **Yes** to validate.

   Connected users are prompted to save their work and log out by a **Maintenance** dialog box. They will be automatically redirected to the login page after 60 seconds

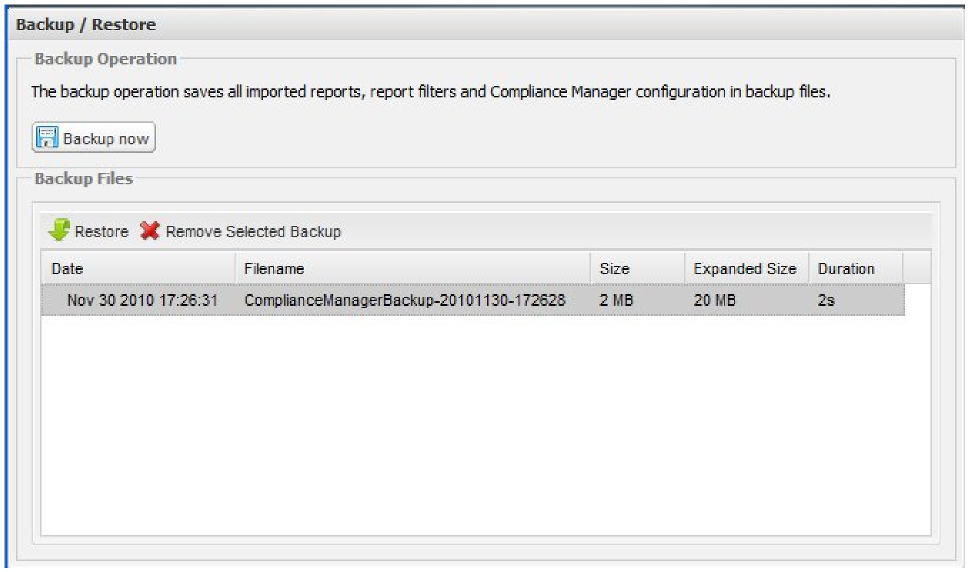
   Maintenance Dialog Box

   The backup of the CM Server database is launched and the backup file is added to the list in the **Backup Files** panel.

   Its filename format is: `ComplianceManagerBackup-<YYYYMMDD>-<HHmmss>`

Backup File Added to the List of Backups



Backup files are stored in the `<LogLogic installation dir>\backups\ directory`.

Restoring a Backup File

Prerequisites

- You must have backed up your database at least once to perform a manual restore.
- Ensure that the image you want to backup is located at `<CM installation dir>\backups`

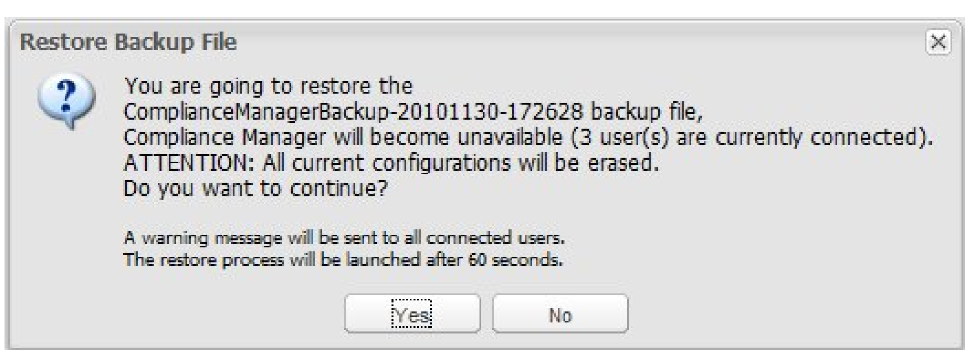
On an MS Windows host, you must close all Windows explorers that might be opened on the `<CM installation dir>` before launching the restore operation.

Procedure

1. Select a backup file from the **Backup Files** panel and click the **Restore** button.

   A **Restore Backup File** dialog box opens asking you to confirm the restore operation.

   Restore Backup File Dialog Box

2. Click **Yes** to validate.

   All connected users are prompted to save their work and log out by a **Maintenance** dialog box.

   The current CM configuration and data are removed, and the CM configuration and data of the selected backup file are restored.

If the backup file does not have a valid format or is not from a supported version, an error message will be displayed.

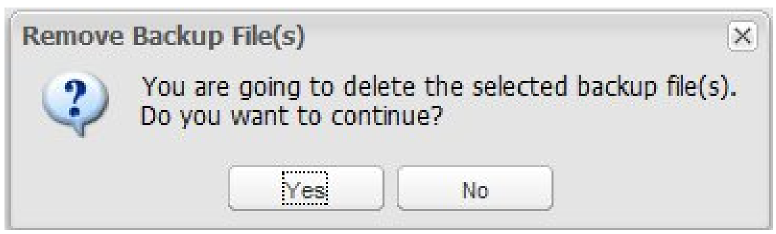
Deleting Old Backup Files

These are the steps to delete old backup files:

Procedure

1. Select one or several backup files from the **Backup Files** panel and click the **Remove Selected Backup** button.

   A **Remove Backup File** dialog box opens asking you to confirm the removal operation.



2. Click **Yes** to validate.

   The backup file(s) is/are deleted.

Appliances

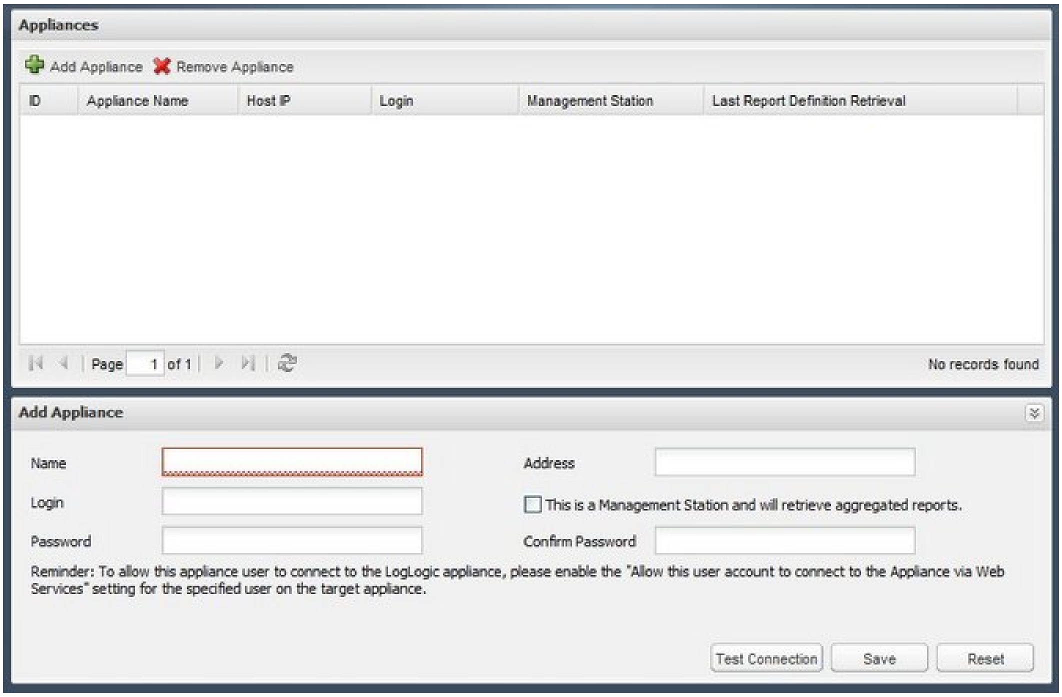
In Administration > Appliances, the CM administrator can add, configure, and remove LX/ST/MX appliances used by LogLogic® Compliance Manager. The Appliance list contains LX/

ST/MX appliance connection information to import report definitions and perform the scheduled report queries.

Contents

Description of the Appliances View

The Appliances view displays two panels - Appliances and Add/Edit Appliance.



Appliances Panel

The top panel, Appliances, displays the list of appliances associated to LogLogic® Compliance Manager. It is from these appliances that CM will retrieve the report definitions which will be used in the whole compliance review cycle.

Appliances Panel Description

Icon	Description
	Opens the **Add Appliance** panel which allows to define the appliance that will be used by CM.
	Allows to delete a selected appliance.
Column	**Description**
ID	The appliance ID generated by CM.
Appliance Name	Displays the name of the appliance
Host IP	Displays the Host IP address of the appliance. It can either be an FQDN or an IP address.
Login	Displays the login of the user account which is allowed to connect the target appliance.

Management Station	Indicates whether the appliance is defined as a Management Station (to retrieve aggregated reports).
Last Report Definition Retrieval	Displays the timestamp of the last report definition retrieval. The timestamp format is YYYY-MM-DD hh:mm:ss

Column Tips

- To sort a column by ascending or descending order, click once on its column header. Sorted columns have a dark grey header and their names are followed either by an upward (ascending) or a downward (descending) arrow.
- To rearrange the order/position of columns, drag-and-drop column headers on the column header row.
- To select the columns that you want to display, click the down triangle arrow on the right hand side of any column header, select the **Columns** menu and tick their corresponding check boxes.
- To resize columns to the desired width, mouseover their column dividers and click-and-drag the left/right arrow.

Add/Edit Appliance Panel

The bottom panel, **Add/Edit Appliance**, allows to define the properties that will be used by LogLogic® Compliance Manager to connect to the appliance.

Add/Edit Appliance Panel Description

Title	Description
Name	A name to refer to the appliance in LogLogic® Compliance Manager.
Address	Host name or IP Address.
Login	A user account defined on the LX/ST/MX appliance which will be used by LogLogic® Compliance Manager to run report queries and import report definitions.
This is a Management Station and will retrieve aggregated reports	If enabled, the LogLogic® Compliance Manager report query for that appliance will be performed across "all appliances" attached to that management station.
Password/Confirm Password	The password for the user account defined on the LX/ST/MX appliance.

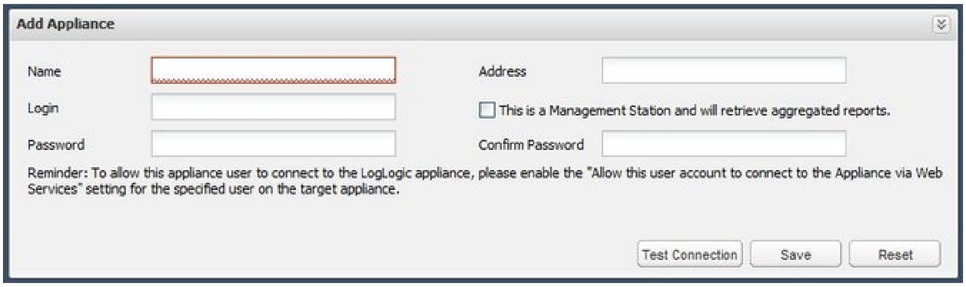
Adding an Appliance

Procedure

1. Select **Administration** > **Appliances** from the navigation menu.

2. Click **Add Appliance**. The **Add Appliance** panel appears at the bottom of the screen

Add Appliance Panel



3. Define the various properties as described in Add/Edit Appliance Panel Description table.

For all LX/ST/MX appliances, the user account that is used to query reports must have the following settings enabled:

LogLogic® Compliance Manager User Account on LX/ST/MX Appliances

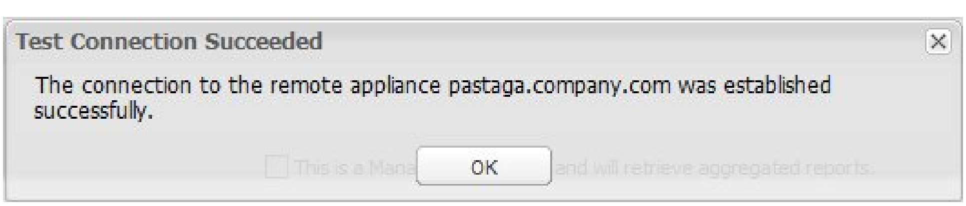
Tab	Action
General	Complete the various fields and tick the **Allow this user account to connect to the Appliance via Web Services** option.
Privileges	Select the following privileges: **Access Custom Reports, Real-time Reports, and Search Archived Data** If the appliance is a Management Station, the user account must also have the **Access Management Station** privilege.
Devices	Any log sources used by your compliance reports must be listed in the **Selected Devices** list. It is good practice to check **Access all devices in the Appliance**.
Appliances	If the appliance is a Management Station, make sure that all the appliances that may be included in any schedules are listed in the **Selected Appliances** list.

4. Optionally, click **Test Connection** to check:

- the network connectivity to the appliance,
- the validity of the login and password for the appliance,
- that the login can run report queries.

It the Test Connection results are successful, a **Test Connection Succeeded** dialog box opens.

Test Connection Succeeded Dialog Box



If the Test Connection results are not successful, it is nevertheless acceptable to save the current settings. Corrections can be performed at a later time.

5. Click **Save** or **Reset** to revert.

   You will be prompted to retrieve report definitions from the newly added appliance. If you click **Yes**, the report definitions will be retrieved.

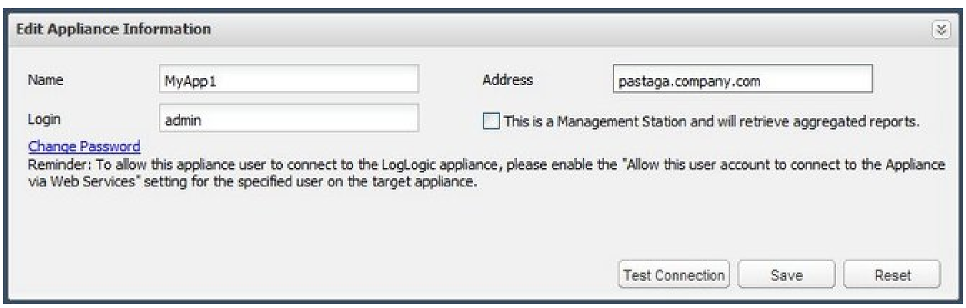
   If you do not want to retrieve report definitions from this appliance at this time, click No. You will be able to retrieve report definitions whenever you want by clicking the Update Report Definitions button in the top panel.

Editing an Appliance

Procedure

1. Select **Administration** > **Appliances** from the navigation menu.
2. Select an appliance in the **Appliances** panel. The account information appears in the **Edit Appliance Information** panel

   Edit Appliance Information Panel



3. In the **Edit Appliance Information** panel, edit the following appliance information: **Name**, **Address**, **Login**, and This is a Management Station and will retrieve aggregated reports checkbox.
4. Optionally, you can click the **Change Password** link to change the password used for the LX/ST/MX appliance Login.
5. Click **Save**.

   The new information has been updated. Otherwise, to revert your entries, click **Reset**.

Retrieving Report Definitions from an Appliance

A report definition retrieval is an action which consists in retrieving all the report definitions of an appliance (to which LogLogic® Compliance Manager is connected). It must be performed regularly to ensure that CM is up-to-date.

Procedure

1. Select **Administration** > **Appliances** from the navigation menu.
2. Select an Appliance.
3. In the **Last Report Retrieval** column, click the **Update Report Definitions** button. A Warning message opens, asking if you want to proceed with the retrieval of report definitions

Warning Message for Import of Report Definitions

4. Click **Yes** to complete the process, otherwise click **No**.

   After the report definitions are retrieved, the number of imported report definitions will be displayed.

> Once report definitions are retrieved, the administrator can map them to Controls in **Review Management** > **Map Reports** to Controls and then schedule reports for review by CM Reviewers.

Sorting Appliances

To filter or sort appliances, move the mouse pointer over the column header row and select the down triangle arrow to display the various applicable filters.

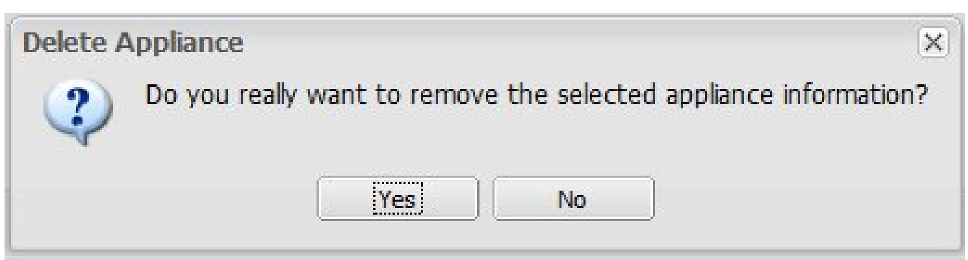
A drop-down list is displayed, which provides the following selections: Sort Ascending, Sort Descending, Columns (ID, Appliance Name, Host IP, Login, Management Station, and Last Report Retrieval).

Removing an Appliance

Procedure

1. Select **Administration** > **Appliances** from the navigation menu.
2. Select one or more appliances.
3. Click **Remove Appliance**.

   A **Delete Appliance** dialog box opens, asking whether you want to delete this appliance.



4. Click **Yes**.

   The appliance is deleted from LogLogic® Compliance Manager.

> - The appliance is also removed from all report schedules set to retrieve reports from it.
> - The imported custom report definitions for the appliance are also removed.
> - Existing retrieved reports are unaffected BUT the hyperlinks that can be foundin all Report tabs are removed, i.e. Source Appliance and Count hyperlinks.

Remote Authentication

LogLogic® Compliance Manager supports the use of Radius and Active Directory server user accounts for authentication. To do so, the administrator must first define these user accounts on the Radius/ Active Directory remote authentication server itself, and then define the remote authentication server in CM (in **Administration** > **Remote Authentication**).

When a user authenticates to CM via the Web UI, CM first consults the local user accounts. If the Login is not found in the local user accounts, CM will then query configured remote authentication servers to authenticate the Login. When the Login is authenticated via Radius/Active Directory, CM will then retrieve the authorized roles for the Login as defined by the Radius/Active Directory server configuration.

If multiple Radius/Active Directory servers are configured, CM will query each server, until one of the servers authenticates the user account Login credentials. If the user account cannot be authenticated using either the local user accounts, or Radius/Active Directory servers, the Login is denied access.

Contents

Defining CM Roles on a Remote Authentication Server

Before configuring a remote authentication server in CM, you must first define the user accounts on the server itself, and assign them the appropriate CM Roles.

LogLogic® Compliance Manager supports Radius and Active Directory remote authentication servers. This section explains how to define CM Roles on these two types of remote servers.

Contents

Defining CM Roles for Radius User Accounts

A Radius vendor attribute, **`LogLogic-CM-Roles`**, is used to define the CM roles for Radius-based user accounts.

For example, with FreeRadius, the configuration to assign all CM roles to user account sampleuser is:

```
sampleuser Auth-Type := Local, User-Password =="<password-for-sample-user>"
```

```
LogLogic-CM-Roles = "ROLE_REVIEWER ROLE_ADMIN ROLE_CIO ROLE_INTERNAL_AUDITOR" [OR]
"ROLE_EXTERNAL_AUDITOR"
```

To assign only the Reviewer role to a Radius user account, the following configuration is used:

```
sampleuser Auth-Type := Local, User-Password =="<password-for-sample-user>"
```

```
LogLogic-CM-Roles = "ROLE_REVIEWER"
```

The values for LogLogic-CM-Roles are the following:

- **`ROLE_REVIEWER`**
- **`ROLE_ADMIN`**
- **`ROLE_CIO`** (for the “Executive” role)
- **`ROLE_INTERNAL_AUDITOR`**
- **`ROLE_EXTERNAL_AUDITOR`**

The two auditor roles i.e., ROLE_INTERNAL_AUDITOR and ROLE_EXTERNAL_AUDITOR are exclusive. Therefore, you cannot assign these two roles to a user account, you have to choose one of them.

Please consult your Radius Authentication Server documentation for specific information about user account vendor attributes.

Role Specification Procedure on FreeRADIUS

Procedure

1. Create a dictionary file.

   Create the file `/usr/share/freeradius/dictionary.loglogic` with the following contents:

   ```
   VENDOR LOGLOGIC 18552

   BEGIN-VENDOR LOGLOGIC

   ATTRIBUTE LogLogic-CM-Roles 1 string

   END-VENDOR LOGLOGIC
   ```
2. Include the dictionary file into the server configuration.

   Edit `/usr/local/shared/freeradius/dictionary` and add the following line in the appropriate section:

   ```
   $INCLUDE dictionary.loglogic
   ```
3. Add the CM role attributes to a user.

   Edit the `/etc/freeradius/users` file to add the new attribute users. The attribute goes on a line below the one with the user name and must be indented. The line has the format:

   ```
   LogLogic-CM-Roles = "<CM role attribute(s)>"
   ```

   where `<CM role attribute(s)>` can be:

   ROLE_REVIEWER

   ROLE_ADMIN

   ROLE_CIO (for the "Executive" role)

   ROLE_INTERNAL_AUDITOR

   ROLE_EXTERNAL_AUDITOR

   You can define several `CM role attributes` for a user account by adding them one after the other separated by blank spaces, e.g., **LogLogic-CM-Roles = "ROLE_CIO ROLE_INTERNAL_AUDITOR"**
4. Restart the freeradius server process.

   Use `kill -9` on the PID and run `/usr/sbin/freeradius`.

   Examples:

   ```
   cio Cleartext-Password := "cio"

   Reply-Message = "Hello, %{User-Name}, you are an executive on this server",

   LogLogic-CM-Roles = "ROLE_CIO"

   rev Cleartext-Password := "rev"

   Reply-Message = "Hello, %{User-Name}, you are a reviewer on this server",

   LogLogic-CM-Roles = "ROLE_REVIEWER"
   ```

```
adm Cleartext-Password := "adm"

Reply-Message = "Hello, %{User-Name}, you are an administrator on this server",

LogLogic-CM-Roles = "ROLE_ADMIN"

cbo4 Cleartext-Password := "cbo4"

Reply-Message = "Hello, %{User-Name}, you are admin & reviewer on this server",

LogLogic-CM-Roles = "ROLE_ADMIN ROLE_REVIEWER"
```

Defining CM Roles for Active Directory User Accounts

To be used by LogLogic® Compliance Manager, Active Directory users must be members of a group whose name starts with the prefix: **ROLE_LOGLOGIC_CM**

Each CM role is then defined by adding one of the following suffixes to the group name:

- **REVIEWER**
- **ADMIN**
- **CIO** (for the “Executive” role)
- **INTERNAL_AUDITOR**
- **EXTERNAL_AUDITOR**

All the groups for which the user is a member will be taken into account (even if the group is part of another group, or if is the primary group).

The two auditor roles i.e., INTERNAL_AUDITOR and EXTERNAL_AUDITOR are exclusive. Therefore, you cannot assign these two roles to a user account, you have to choose one of them.

Please consult your Active Directory Authentication Server documentation for specific information about user account attributes.

To assign the Reviewer and the CIO (Executive) roles to an Active Directory user account:

Procedure

1. Create the two following groups on the AD server:

   ROLE_LOGLOGIC_CM_REVIEWER

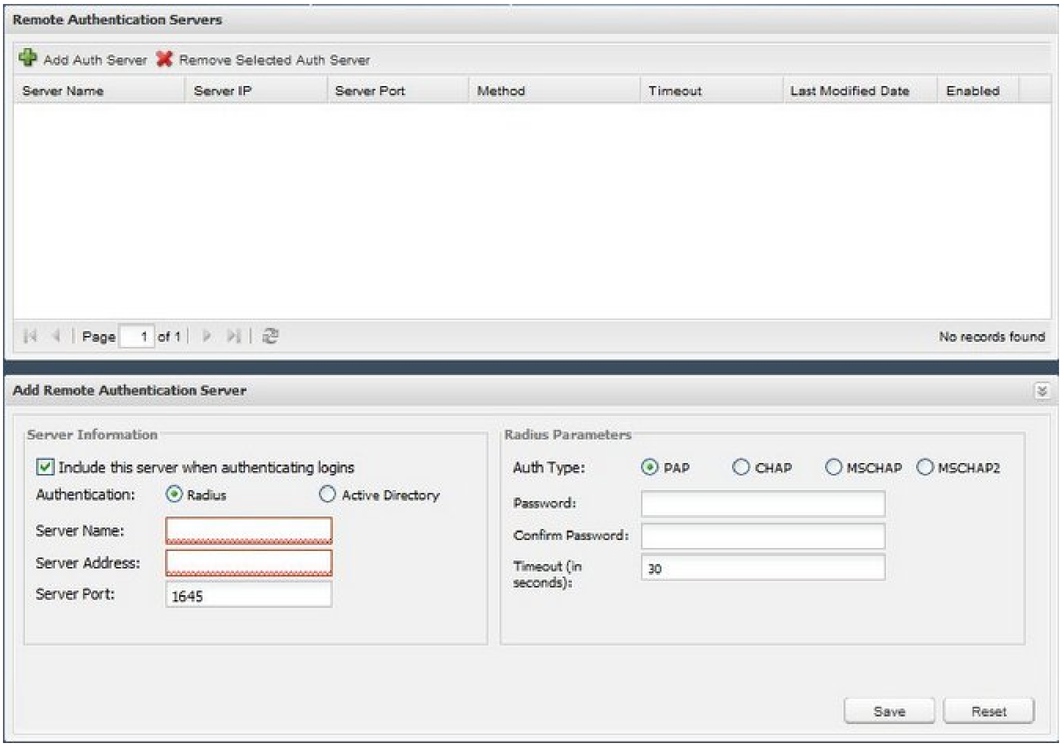
   ROLE_LOGLOGIC_CM_CIO

2. Add the user account as a member of these two groups.

Description of the Remote Authentication Servers View

The Remote Authentication Servers view displays two panels, i.e., Remote Authentication Servers and Add/Edit Remote Server

Remote Authentication View



Remote Authentication Servers Panel

The top panel, **Remote Authentication Servers**, displays the list of remote authentication servers associated to LogLogic® Compliance Manager.

Icon	Description
	Opens the Add Remote Authentication Server panel which allows to define the remote server that will be used by CM.
	Allows to delete a selected remote server.
Column	**Description**
Server Name	Indicates the name of the server
Server IP	Indicates the host IP address of the server.It can either be an FQDN or an IP address.
Server Port	Indicates the port of the remote Server.

Icon	Description
Method	Indicates the selected server type and the selected authentication method with the following format: `<Server Type> / <Auth Type>` For a Radius server, you can have: • Radius / PAP • Radius / CHAP • Radius / MSCHAP • Radius / MSCHAP2 For an Active Directory server, you can have: • Active Directory / Kerberos • Active Directory / Simple
Timeout	Indicates the amount of time, in seconds, that LogLogic® Compliance Manager will wait for a response from the remote authentication server before abandoning an authentication request.
Last Modified Date	Displays the timestamp of the last modification performed in CM for the remote server. The timestamp format is YYYY-MM-DD hh:mm:ss
Enabled	Indicates whether the remote server is enabled or not in CM, that is to say whether the **Include this server when authenticating logins** option is enabled in the **Add/Edit Remote Server** panel.

Column Tips

- To sort a column by ascending or descending order, click once on its column header. Sorted columns have a dark grey header and their names are followed either by an upward (ascending) or a downward (descending) arrow.
- To rearrange the order/position of columns, drag-and-drop column headers on the column header row.
- To select the columns that you want to display, click the down triangle arrow on the right hand side of any column header, select the **Columns** menu and tick their corresponding checkboxes.
- To resize columns to the desired width, mouseover their column dividers and click-and-drag the left/right arrow.

Add/Edit Remote Authentication Server Panel

The bottom panel, **Add/Edit Remote Authentication Server**, allows to define the properties that will be used by LogLogic® Compliance Manager to connect to the remote authentication server.

Title	Description
Include this server when authenticating logins	If this checkbox is ticked, the remote authentication server will be used for authenticating Logins.

Title	Description
Authentication	Allows to define the type of the remote authentication server, i.e., Radius or Active Directory. Several properties vary accordingly.
Server Name	Indicates the name of the remote authentication server.
Server Address	Indicates the host name or IP address of the remote authentication server.
Server Port	Indicates the port of the remote authentication server.
Radius Parameters	
Auth Type	Indicates the selected authentication type: • PAP • CHAP • MSCHAP • MSCHAP2
Password/Confirm Password	A secret password defined on the remote authentication server for your LogLogic® Compliance Manager to authenticate with this server.
Timeout (in seconds)	The amount of time, in seconds, that LogLogic® Compliance Manager will wait for a response from the remote authentication server before abandoning an authentication request.
Active Directory Parameters	
Auth Type	Indicates the selected authentication type: • Kerberos • Simple Authentication If **Simple Authentication** is selected you will have to define the NT Domain property (see below).
Realm	Indicates the Active Directory trust realm name

<table>
<tr><th>Title</th><th>Description</th></tr>
<tr><td>NT Domain</td><td>Indicates the NT Domain name.

This name should not exceed 15 characters and should not contain the following characters (between square brackets):

[\ ]
[/]
[:]
[*]
[?]
[,]
[<]
[>]
[|]</td></tr>
<tr><td>Test</td><td>Use this button to test the connection between LogLogic® Compliance Manager and the Remote Active Directory.</td></tr>
</table>

Adding a Remote Authentication Server

After you have defined user accounts on the remote authentication server itself (see Defining CM Roles on a Remote Authentication Server), you can proceed with the configuration of this server in LogLogic® Compliance Manager.

Procedure

1. Select **Administration** > **Remote Authentication** from the navigation menu.
2. In the **Remote Authentication Servers** panel, click **Add Auth Server**.
   The **Add Remote Authentication** Server panel opens.
3. Set the various properties of the Server **Information** pane.

   Server Information Pane Properties

Setting	Description
Include this server when authenticating logins	Select this box to use this remote authentication server for authenticating Logins.
Authentication	
Server Name	Enter a unique name for your remote authentication server.
Server Address	Enter a host name or IP address for the remote authentication server.
Server Port	Enter the port for the remote authentication server.

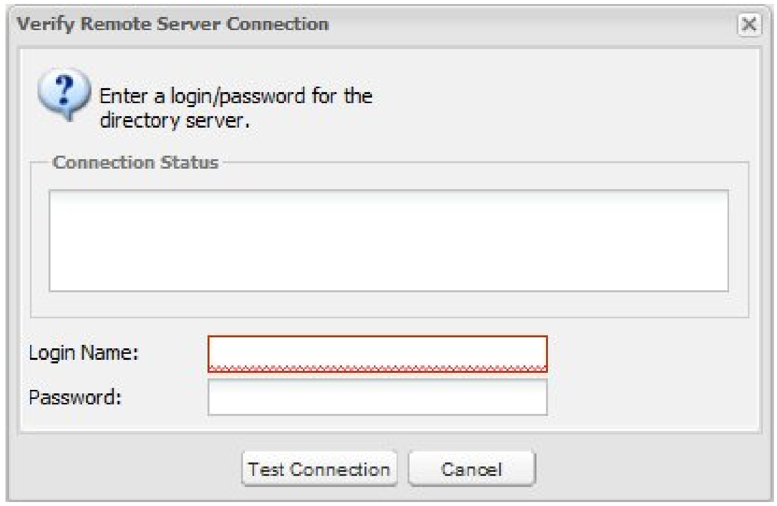
4. Set the various properties of the **Radius/Active Directory Parameters** pane.

Radius/Active Directory Parameters Pane Properties

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td colspan="2">Radius Parameters</td></tr>
<tr><td>Auth Type</td><td>Indicates the selected authentication type:
• PAP
• CHAP
• MSCHAP
• MSCHAP2</td></tr>
<tr><td>Password/ Confirm Password</td><td>A secret password defined on the remote authentication server for your LogLogic® Compliance Manager to authenticate with this server.</td></tr>
<tr><td>Timeout (in seconds)</td><td>The amount of time, in seconds, that LogLogic® Compliance Manager will wait for a response from the remote authentication server before abandoning an authentication request.</td></tr>
<tr><td colspan="2">Active Directory Parameters</td></tr>
<tr><td>Auth Type</td><td>Indicates the selected authentication type:
• Kerberos
• Simple Authentication
Note: If Simple Authentication is selected you will have to define the NT Domain property (see below).</td></tr>
<tr><td>Realm</td><td>Indicates the authentication name (i.e. realm)</td></tr>
<tr><td>NT Domain</td><td>Indicates the NT Domain name.
This name should not exceed 15 characters and should not contain the following characters (between square brackets):
[\]
[/]
[:]
[*]
[?]
[,]
[<]
[>]
[|]</td></tr>
</table>

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td>Test</td><td>Use this button to test the connection between LogLogic® Compliance Manager and the Remote Active Directory server.

A Verify Remote Server Connection dialog box opens, prompting you to enter login/password. Enter your credentials and click the Test Connection button.


</td></tr>
</table>

5. Click **Save**. To revert, click **Reset**.

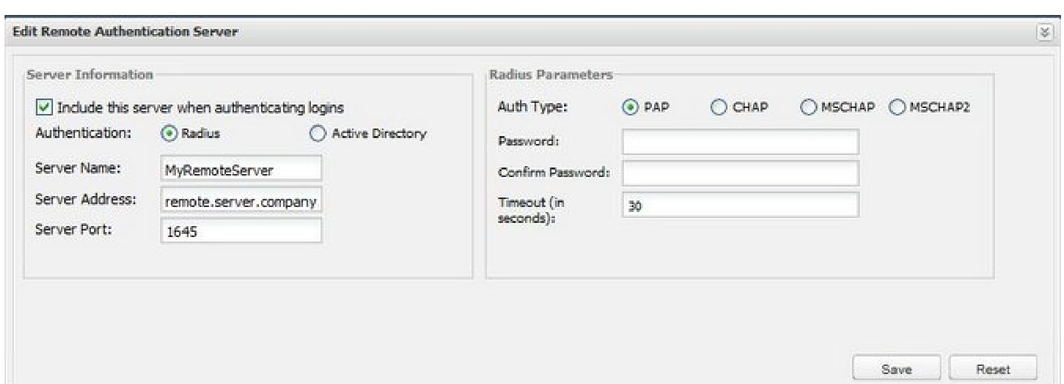
Editing a Remote Authentication Server

Procedure

1. Select **Administration** > **Remote Authentication** from the navigation menu.
2. Select a server.

   The remote authentication server information appears in the **Edit Remote Authentication Server** panel.

   Edit Remote Authentication Information Panel



3. Edit the **Server Information** pane properties.
4. Edit the **Radius/Active Directory Parameters** pane properties.
5. Click **Save**.
   The remote authentication server properties are updated. Otherwise, to revert your entries, click **Reset**.

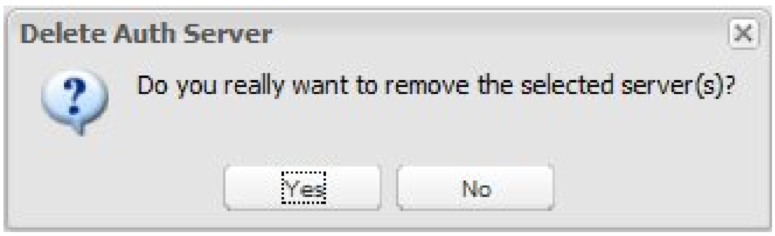
Removing a Remote Authentication Server

Procedure

1. Select **Administration** > **Remote Authentication** from the navigation menu.
2. Select one or more servers.
3. Click **Remove Selected Auth Server**.

   A **Delete Radius** dialog box opens, asking you to confirm the removal of the selected server(s).

   Delete Radius Dialog Box

4. Click **Yes**.

> The **Include this server when authenticating logins** checkbox is useful if you want to temporarily disable the querying of a Radius server, but do not want to remove the server configuration. For example, if you need to configure two servers for redundancy, you might disable the first server while verifying settings for the second server.

Sorting Remote Authentication Servers

To filter or sort remote authentication servers, move the mouse pointer over the column header row and select the down triangle arrow to display the various applicable filters.

A drop-down list is displayed, which provides the following selections: **Sort Ascending**, **Sort Descending**, **Columns** (Server name, Server IP, Server port, Method, Timeout, Last Modified Date, and Enabled).

Glossary

Glossary of Terms

Term	Definition
Activity	An activity refers to any compliance related task including scheduling reports and the review workflow process until the report is marked as a completed task. For example, report schedules and review operations.
Administrator (role	The Administrator is responsible for installing and configuring the LogLogic® Compliance Manager. An administrator is someone who understands the compliance mandates and controls and is able to schedule reports that are used to manage the control objectives. The Administrator can: • Enable the compliance review process by scheduling reports and specifying reviewers for the report results • Manage users and roles • Review LogLogic® Compliance Manager application history • Configure system wide settings for the LogLogic® Compliance Manager appliance • Manage the mandates and controls by creating custom ones and enabling the mandates or the controls relevant for the organization compliance scope. In LogLogic® Compliance Manager, their primary work areas are the **Review Management** and the **Administration** menus.
Appliance	LogLogic hardware that collects and captures log data on a network. There are several Appliance product families (LX, ST, MX, MA) that address different needs for message collection and storage. In LogLogic® Compliance Manager, appliances must be defined so that the application can connect to them and retrieve compliance reports. The collected report definitions are then mapped to specific regulatory control objectives.
Auditor (role)	A user who is given this role by the Administrator, has an at-a-glance view of the Review process for the associated mandate. The auditor both validates the compliance to mandates and checks that the LogLogic® Compliance Manager review process is correctly applied by the various CM users. A distinction is made between the **Internal Auditor Role** and the **External Auditor Role**. The Internal Auditor's role is to prepare his/her organization to a compliance audit made by an External Auditor. These two roles actually have the same abilities, except that the External Auditor cannot write comments. This functionality is indeed reserved to the Internal Auditor whether to point out specific things to the Reviewers. In LogLogic® Compliance Manager, their work area is the *Audit Dashboard*.
Control	A control is a specific requirement that must be checked and verified, sometime s by external auditors. A mandate contains a large number of controls, there can be several hundreds of them. A Control holds several compliance report definitions (see "Report definition").

Term	Definition
Dashboard	A dashboard is a user interface that organizes and presents information in a way that is easy to read. LogLogic® Compliance Manager offers three different dashboards, i.e., Executive, Review and Audit dashboards.
Executive (role)	A user with this role has an at-a-glance view of the timeliness of the compliance activities and ratings which includes the assessment by the compliance team. In LogLogic® Compliance Manager, their work area is the *Executive Dashboard*.
Mandate	A mandate can represent a government regulation (e.g., SOX), an industry regulation (e.g., PCI), a best practice framework (e.g., ISO) or a set of internal regulatory constraints enforced in the organization. It typically contains a list of requirements that an organization must satisfy. Mandates typically contain many controls (see "Control" definition).
Month to Date (MTD)	A predefined observation period that can be used in Dashboards to assess the report review progress from the beginning of the month up to the current date.
Overdue Tasks	Overdue tasks are tasks that have crossed their due date, that is to say, the date when they were supposed to be complete. In the Overdue Tasks module of the Executive Dashboard, the executive user can view the overdue tasks distribution by user and determine the reviewers who are late.
Quarter to Date (QTD)	A predefined observation period that can be used in Dashboards to assess the report review progress from the beginning of the quarter up to the current date. The beginning of the quarter is related to the **Financial Year Starting Date** defined in **Administration > General Settings**.
Rating	The rating of a report indicates its degree of importance/criticality. It allows to flag the importance granted to the report visually through a color code where: • Grey signals that there is no rating (no impact). • Green signals that the rating is low (minimal impact). • Orange signals that the rating is medium (some impact). • Red signals that the rating is high (high impact).
Report	A report is activity log data (e.g., user escalations, firewall ports used, denied traffic, etc.) retrieved from a LogLogic appliance, and organized into an easy to understand format. It contains information which must be reviewed, approved, flagged, and/or escalated by the Reviewer(s). It is an instance of a report definition generated on a remote LMI appliance.
Report definition	In LogLogic® Compliance Manager, a report definition is mapped to a mandate control by the administrator. Once the schedule and review management are defined for a report definition, instances of this report definition (i.e., reports) will be generated whenever information is retrieved from an appliance.

Term	Definition
Report definition retrieval	A report definition retrieval is an action which consists in retrieving all the report definitions of an appliance (to which LogLogic® Compliance Manager is connected). It must be performed regularly in **Administration > Appliances**, to ensure that CM is up-to-date.
Report result	Report results can be considered as summary views of similar report rows (referred to as "report result details"). They are displayed in the Report tab when a report is selected above, in the list of reports.
Report result detail	A report result detail contains the list of messages detailing a specific report result. These messages are retrieved from a remote LMI appliance when the user clicks on the number displayed in the "Count" column of a report result.
Report schedule	A report schedule can be compared to a task generator. Each generated task contains a schedule phase and a review phase. During the schedule phase, a report query is sent on one or several appliances to retrieve LMI report data at a precise time of the day*, depending on a query time range. The query time range can have a Daily, a Weekly or a Monthly frequency and always ends at midnight on the day that precedes the schedule phase. The aim of this schedule mechanism is therefore to retrieve report data on a continuous way even if its retrieval relies on segmented query time ranges. * The task might not be executed at that very precise time of the day because all tasks are scheduled at the same time and they are processed one after the other. Once the schedule phase is complete, the review phase begins. The report reviewers have to make a review of the report data retrieved during the schedule phase, respecting a due date.
Review Status	The review status gives the current status of the report review, i.e., on time, approaching due date or past due date. • On-time: The report review is on-time regarding the due date. • Approaching Due Date: The report review is very close to the due date. The default time allowed before a review is given a yellow status is 80% of the elapsed time between the Creation date and the Due date. This threshold can be changed in General Settings. • Past Due: The report review is over the due date.
Reviewer (role)	A user with this role performs detailed research and analysis. A Reviewer is required to periodically (daily or on an alternate regular schedule) review reports. They are also delegated the investigation tasks and are responsible for preparing summarized information for executives. The Reviewer provides the critical human intelligence to identify and guide the organization compliance process. In LogLogic® Compliance Manager, the work area of Reviewers i is the *Review Dashboard*.

Term	Definition
State	The state gives information about the current state of a report review task. • Ready for Review: A report has been retrieved from an appliance. It is ready to be reviewed by its primary reviewer. • In Review: The report is currently being reviewed either by its primary reviewer or its final reviewer. • Returned: The report has been returned by the final reviewer to the primary reviewer. • Complete: The report has been reviewed by the reviewers.
Syslog	A log forwarding standard and protocol, used to tranmist log messages via UDP or TCP.
Year to Date (YTD)	A predefined observation period that can be used in Dashboards to assess the report review progress from the beginning of the year up to the current date. The beginning of the year is related to the **Financial Year Starting Date** defined in **Administration > General Settings.**