Rwanda Integrated Electronic Case Management System

Rwanda IECMS

SETTINGS

ADMINISTRATOR’S GUIDE

Version 1.0

SYNERGY
INTERNATIONAL SYSTEMS

TABLE OF CONTENTS

TABLE OF FIGURES

INTRODUCTION

This document describes the *Settings* section in the *Rwanda Integrated Electronic Case Management System (Rwanda IECMS)* application developed for the Justice, Reconciliation, Law and Order Sector (JRLOS) of Rwanda*.* It provides the necessary instructions which the administrators and/or users granted with administrative rights should follow in order to ensure successful application management. Use of this documents and compliance with the standards specified herein is mandatory for anyone working with the mentioned application.

OVERVIEW

The *Integrated Electronic Case Management System for Rwanda (Rwanda IECMS)* is an automated information management system, which is designed within the initiative of modernizing Rwanda's Justice, Reconciliation, Law and Order Sector (JRLOS). It is intended to ensure improved access to and transparency of justice information both for the government institutions and general public. Moreover, the system aims at facilitating information sharing at key decision points, as well as to improve efficiency and coordination of the police, prosecution, and court activities in the Republic of Rwanda. Furthermore, it is intended to replace the paper-based case records and static spreadsheets and workflows with their computerized counterparts in order to enable full reproduction of cases along with case proceeding information in the event of loss or physical damage of the case file.

The main objective of *Rwanda IECMS* is to serve as a centralized and unique database for all justice sector institutions, including the Rwanda National Police (RNP), National Public Prosecution Authority (NPPA), Rwanda Judiciary (RJ), and Rwanda Correctional Services (RCS). Also, it is a sector-wide platform to assist all the officials accessing the system to have an easy and ad-hoc access to the information required for processing the cases and implementing day-to-day operations. *Rwanda IECMS* is intended to help to standardize case record information storage and to streamline current processes, and, thus, ensure more effective follow-up at different levels. It is also the main database and data collection and reporting system as it guarantees effective access to the case data, promotes accountability, and increases public trust and confidence.

Rwanda IECMS consists of the following applications, each dedicated to one justice agency and used to handle their business processes:

- Rwanda National Police

- Rwanda National Public Prosecution Authority
- Rwanda Judiciary
- Rwanda Correctional Service
- Civil Litigation Service

Rwanda IECMS incorporates business intelligence and data management solutions with comprehensive application administration functions. As such, it is equipped with a number of administrative tools, which aim at providing the application administrators with the possibility of performing their daily assignments in an easily manageable way.

The administrative tools available in *Rwanda IECMS* are intended to help make the entire application management process more intuitive and manageable. All the administrative tools are available to the system administrators and advanced users in the *Settings* section. The *Settings* section in *Rwanda IECMS* is a browser-based user interface allowing the system administrators to manage the application and all its instances, including users, categories, login policies, system configurations, etc. Moreover, using the tools that the *Settings* section offers, the administrators can control the application functions and resources available to users and user groups. They can also carry out their daily assignments in the most efficient and effective manner possible.

Rwanda IECMS provides a web-based user interface and requires having a web browser pre-installed.

SETTINGS SECTION

This chapter describes the *Settings* section within *Rwanda IECMS* that provides a comprehensive toolkit for administering, monitoring, and evaluating the application resources. Moreover, with the help of the tools found in the *Settings* section, you can easily manage the internal system configurations, including setting up user accounts, monitoring user activity in the application in order to prevent the system from crashing, define user access policies and permissions, etc.

The *Settings* section encompasses the following tools and components:

- **Workflow** – for managing workflow based processes through an embedded workflow designer;
- **Data Management –** for managing categories and their items;
- **Configuration** – for managing system configurations;
- **User Management** – for managing users, roles, and user groups;
- **Policies –** for managing system policies;
- **Monitoring** – for managing sessions and locks;
- **Audit –** for auditing system security, notifications, etc.;
- **Personal –** for managing user profile details.

The chapters below will provide detailed descriptions of each of the tools available, as well as will give step-by-step instructions on how to interact with them.

Accessing the Settings Section

The *Settings* section is intended for the application administrators or advanced users granted with the administrative privileges. For accessing the *Settings* section, click the respective icon in the application header and select the tool that you are intending to use (Figure 1).

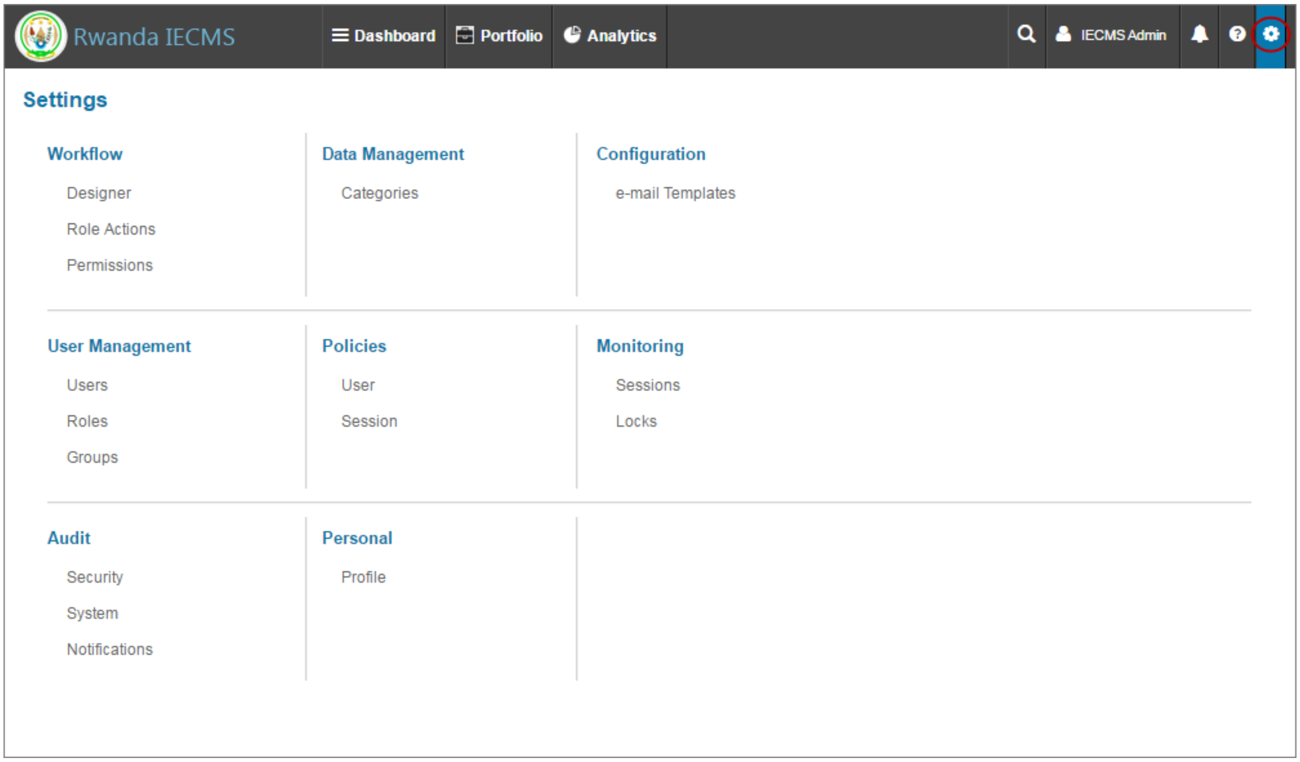

Figure 1: Settings Section

Working in the Settings Section

This chapter will outline what actions you can take in the different consoles that the *Settings* section is incorporated with.

Viewing the Sub-section Item Details

In order to view of sub-section item details, follow the steps below:

1. Go to **Settings → [Console] → [Sub-section]…**
2. Click the item name for which the information needs to be viewed. The details of the selected sub-section item will be displayed on the screen (Figure 2).

To go back to the section where all items are listed, you can make use of the navigation control (breadcrumb trail) found at the top of the screen.

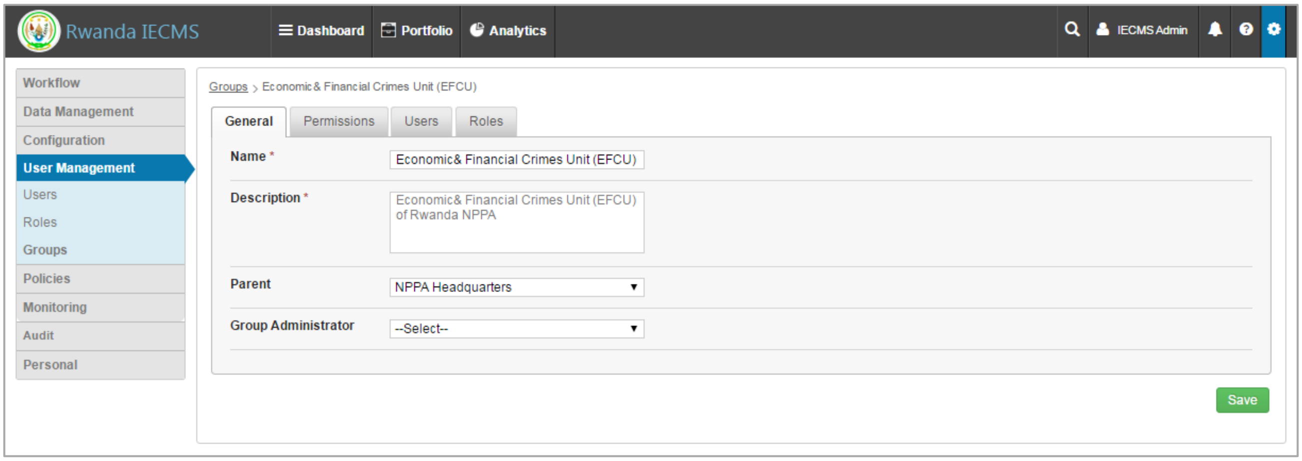

Figure 2: Viewing Details of the Selected Item

Searching for Sub-section Items

One of the primary challenges that users of any project information management system face is the ability to drill down the wealth of the data stored in the application and find the piece of information that they are looking for within a mere fraction of time. This is the reason why the different consoles and sub-sections in the *Settings* section have been enhanced with a built-in comprehensive search mechanism intended for locating sub-section items or any related information matching search criteria easily and instantly.

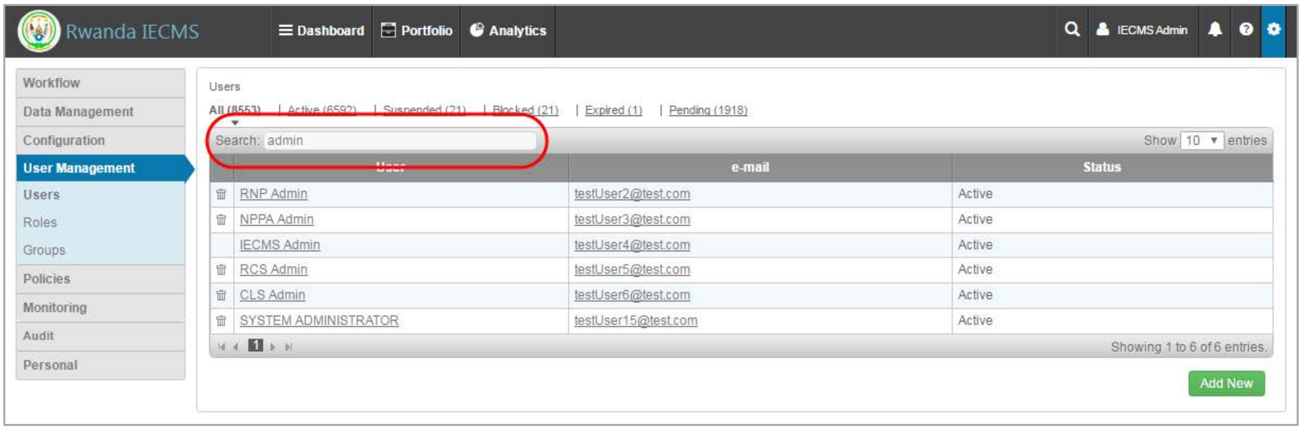

Figure 3: Searching for an Item

The search mechanism available in the *Settings* section allows locating any piece of information within the integrated content based on the keyword search criteria. The search mechanism enables matching capabilities using single words and phrases.

In order to search for sub-section items, follow the steps below:

1. Go to **Settings → [Console] → [Sub-section]…**
2. Type the keyword into the search box. Please, note that the search engine will return all the data that contains any of the letters or numbers you have typed (Figure 3).

Defining the Sorting Order for Sub-section Items

In the *Settings* section, you have the possibility of sorting the items listed in each sub-section of the administrative consoles alphabetically in ascending or descending order.

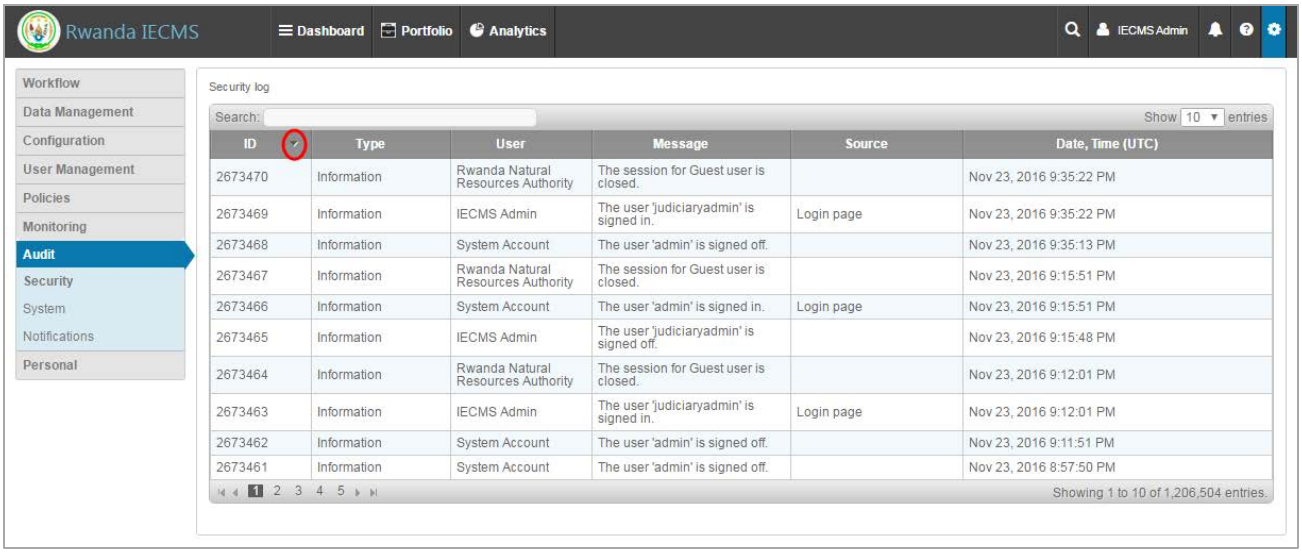

Figure 4: Defining Sorting Order for Session Items

In order to define the sorting order for the sub-section items, follow the steps below:

1. Go to **Settings → [Console] → [Sub-section]…**
2. Click the arrow that appears in the header of the column according to which you want to sort the sub-section items.
3. Click the arrow once again to sort the items in the list in reverse order (Figure 4).

Browsing Pages

The items available in different sub-sections of the administrative consoles are arranged into pages to ensure fast loading and easy navigation.

In order to browse among the pages in each sub-section, follow the steps below:

1. Go to **Settings → [Console] → [Sub-section]…**

2. Click the link of the page number you want to navigate to. You can also use the **Previous** and **Next** as well as **First** and **Last** arrows to move to the required page (Figure 5).

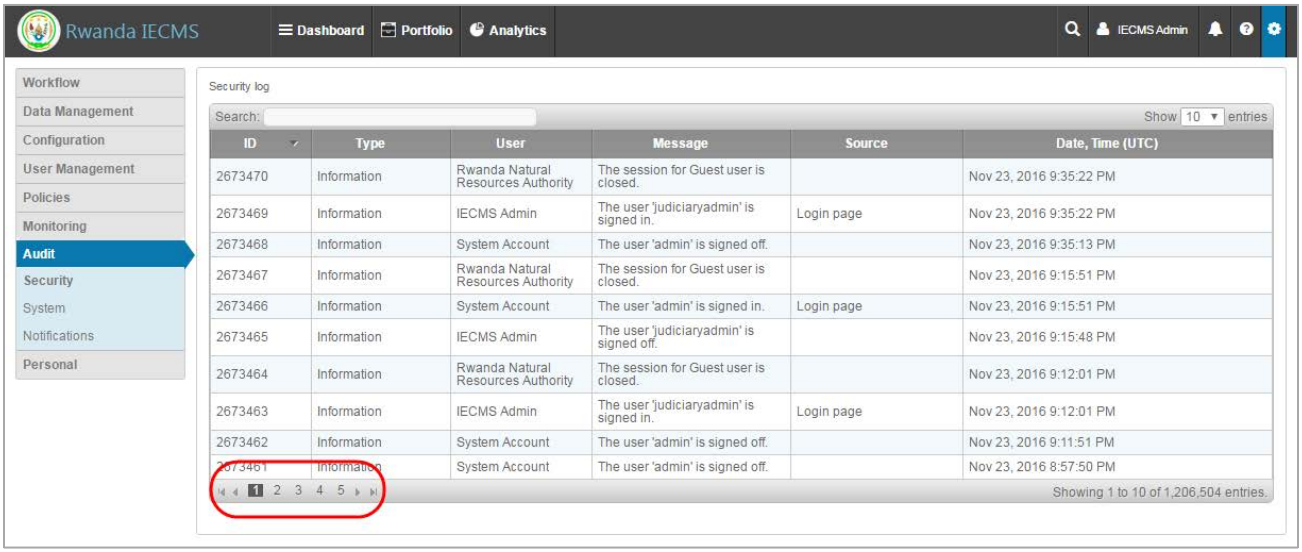

Figure 5: Browsing Pages

Setting the Number of Entries per Page

By default, each sub-section is set to display ten entries per page to ensure fast page loading. However, you can define to view a greater number of entries per page. Please, note that setting a higher number of entries to display on each page can potentially impact page load time since you will load more data with each page.

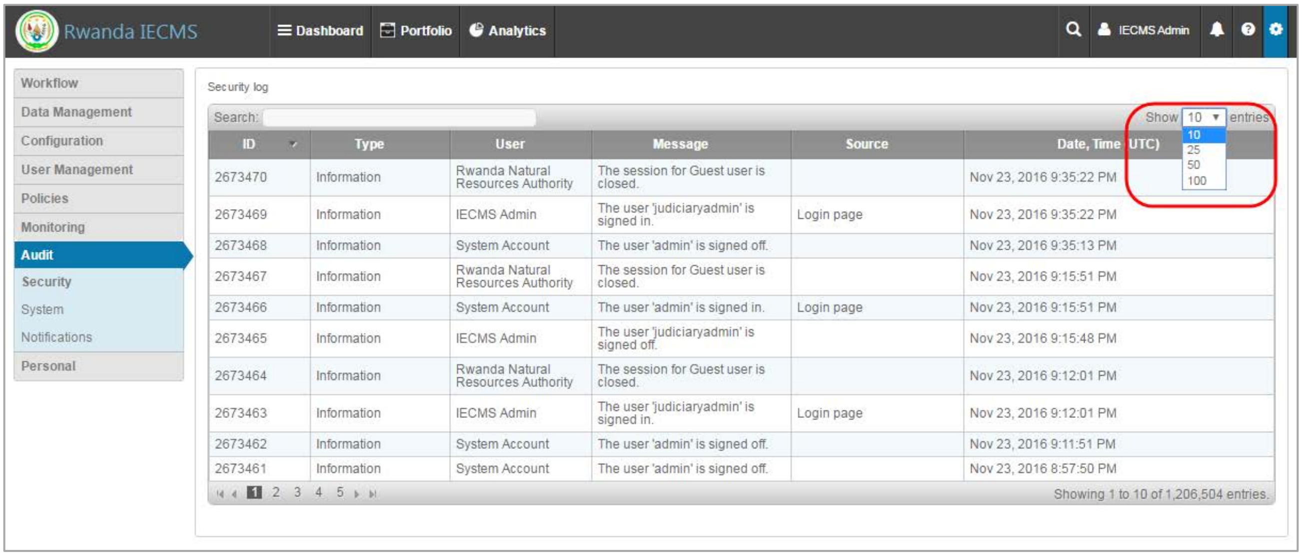

Figure 6: Setting the Number of Entries per Page

In order to set the number of entries per page, follow the steps below:

1. Go to **Settings → [Console] → [Sub-section]…**
2. Select the preferred number from the **Show…entries** drop-down list in the upper right corner of the section table. The exact number of items will immediately be displayed on the screen according to your selection (Figure 6).

Note: Even if you limit the number of displayed items within the table, the simple search tool will find the searched element from the entire list of items.

WORKFLOW CONSOLE

For more details on how to manage the workflow based processes that the application is incorporated with, refer to the *Rwanda IECMS Workflow Management Administrator's Guide* in REFERENCES.

DATA MANAGEMENT CONSOLE

For details on how to perform category management functions, refer to the *Rwanda IECMS Data Management Administrator's Guide* in REFERENCES.

CONFIGURATION CONSOLE

This chapter describes the *Configuration* console under the *Settings* section, where you can set up and manage the application configurations. For instance, you can create **e-mail templates** for the notifications to be sent out.

Accessing the Configuration Console

For accessing the *Configuration* console, go to Settings → Configuration (Figure 7).

The *Configuration* console consists of the following sub-section:

- **e-mail Templates** – to manage the application e-mail templates (see Managing e-mail Templates);

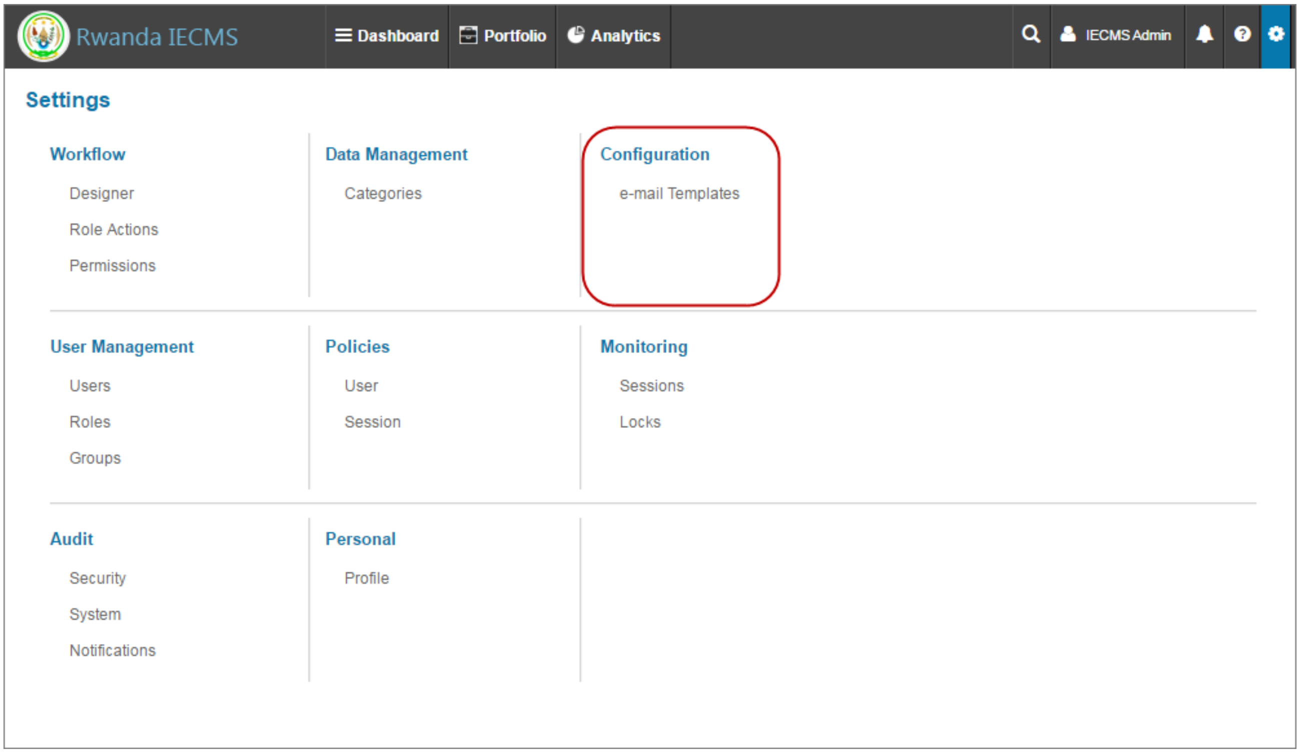

Figure 7: Configuration Console

Managing e-mail Templates

Notifications play an important part in modern applications as they allow the administrators to communicate essential pieces of information to application users via email. Notifications allow the application users to stay informed about the predefined events that can be triggered either by the user or system. Examples of these events include but are not limited to:

- Alerting the user when the system is set under maintenance;
- Informing the user that they have successfully passed the registration process and send them their account information;
- Inform the user about the password change and send them the new password.

The notification text is a template that can include some variables that are replaced with text when the message is sent. They can be used to personalize notifications and provide more detailed information to the user. These fields are surrounded by brackets (<...>).

Templates are managed and configured in the *e-mail Templates* sub-section of the *Configuration* console which can be accessed at Settings → Configuration → e-mail Templates.

Once you access the sub-section, you will be presented with the list of existing templates. The information displayed for each template includes the following:

Component Name	Description
ID	This is an identification number assigned to the template and used for referential purpose.
Name	This is a name assigned to the template.

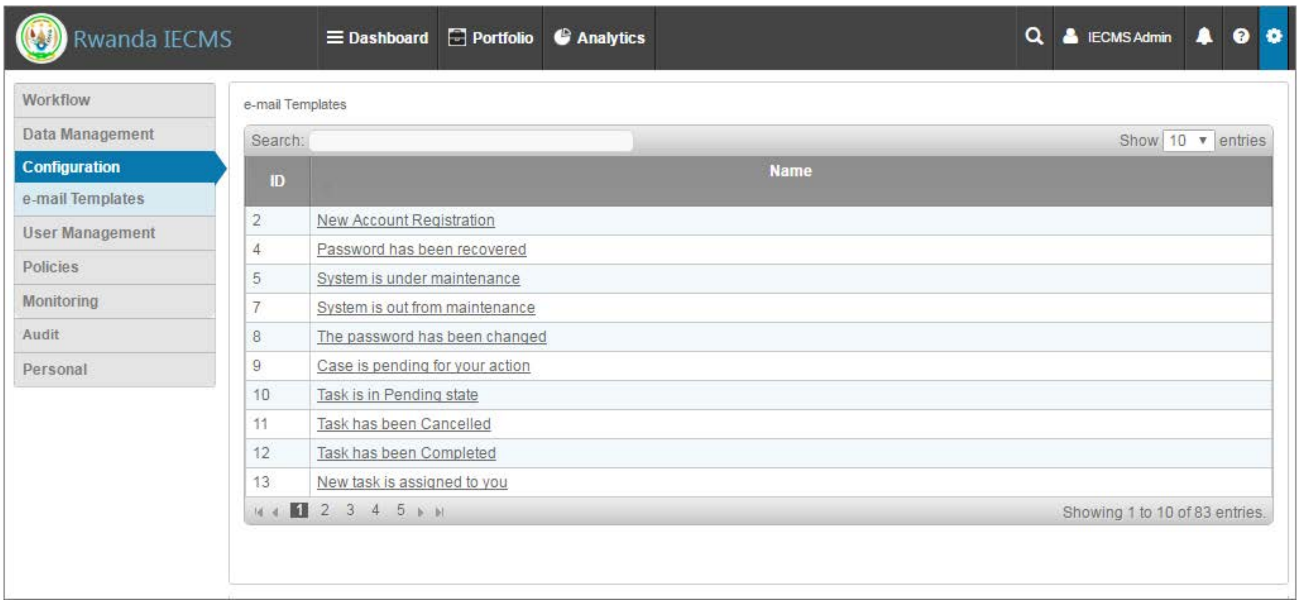

Figure 8: e-mail Templates Sub-section

Configuring e-mail Templates

Notification text can be modified to suit your organization's requirements.

In order to configure a notification template, follow the steps described below:

1. Go to **Settings → Configuration → e-mail Templates…**
2. Click the e-mail template name to configure. You will be directed to the *Edit e-mail Template* page where the selected template details will be displayed (Figure 9).
3. Provide the **Name** for the e-mail template. *This field is mandatory*.
4. Define the **Type** of the e-mail template by ticking all the checkboxes that apply. *This field is mandatory*. The following options are available:

- Notification
- Email
- SMS

Note: If you select the template to be both a notification and an e-mail / SMS, you can tick the same as notification checkbox for the e-mail / SMS to have the same information indicated for the notification. If the contents of the notification and e-mail / SMS are not the same, you should indicate them separately.

5. Specify the notification / e-mail **Subject**. *This field is mandatory*.
6. Provide the notification / e-mail / SMS **Body**. *This field is mandatory*.
7. Click the **Save** button to keep the e-mail template configuration. Or, click the **Cancel** button to discard the modifications made.

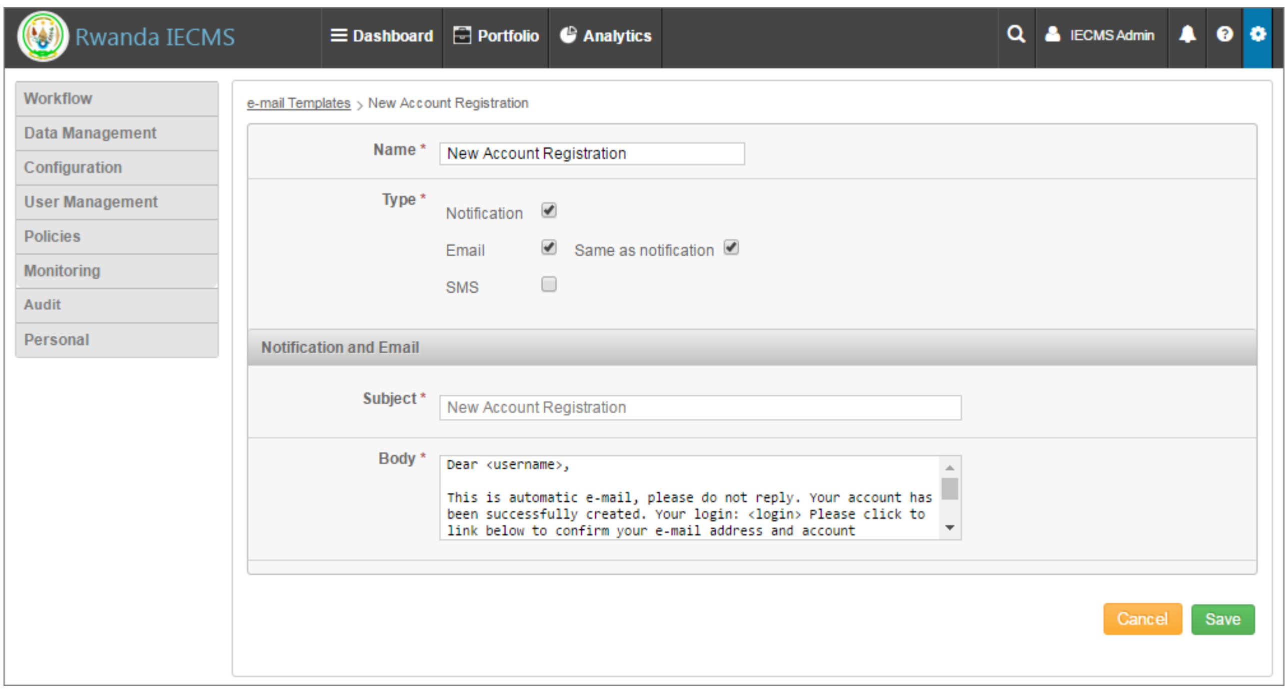

Figure 9: Editing an e-mail Template

Note: Each template has a different list of parameters. For more details, see APPENDIX I: E-MAIL TEMPLATE PARAMETERS.

USER MANAGEMENT CONSOLE

For details on how to perform user management functions, refer to the *Rwanda IECMS User Management Administrator's Guide* in REFERENCES.

POLICIES CONSOLE

This chapter describes the *Policies* console under the *Settings* section, where policies on **User** and **Session** are managed.

Accessing the Policies Console

For accessing the *Policies* console, go to Settings → Policies (Figure 10).

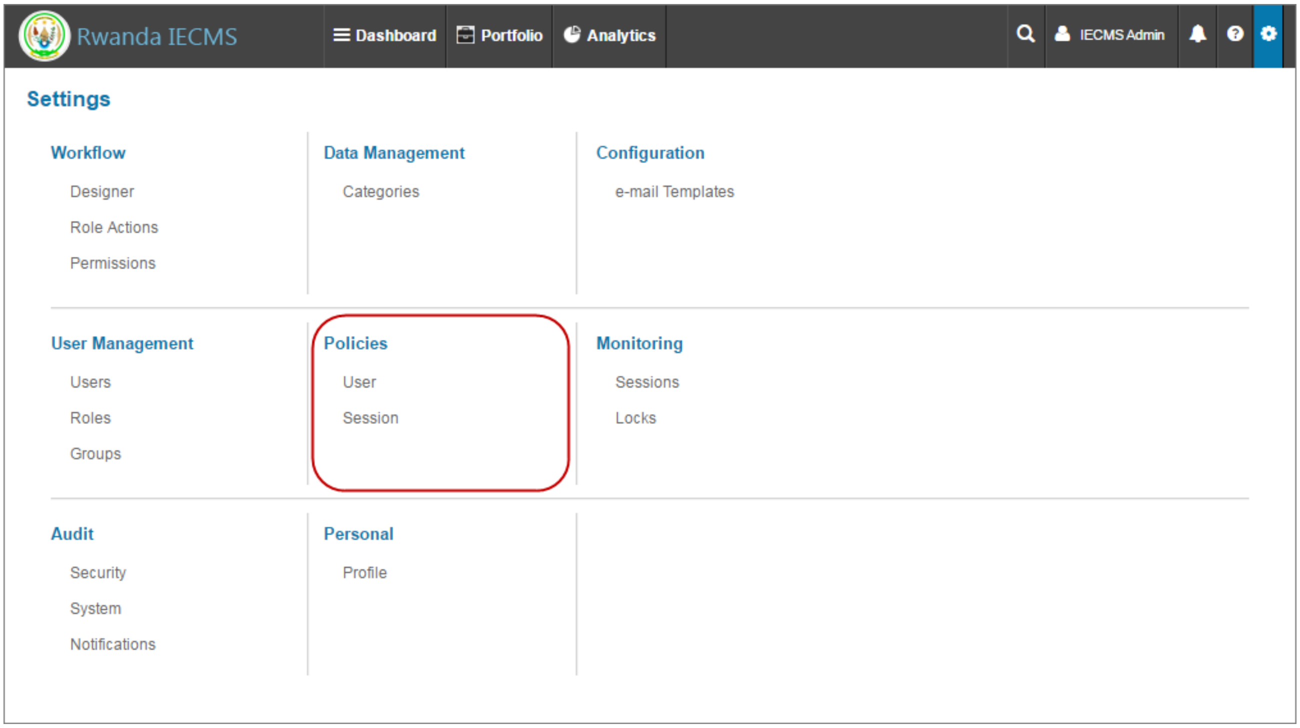

Figure 10: Policies Console

The *Policies* console consists of the following sub-sections:

- **User** – to establish the principles of composition, transmission, and aging for usernames and passwords (see Managing User).

- **Session** - to configure session management policies (see Managing Session).

Managing User

This chapter outlines how you can manage usernames and passwords. They are an important aspect of application security as they are in the front line of protection for the accounts of users accessing the application. This is why it is necessary to establish standards for behavior in naming and operating user accounts as well as for creating strong passwords and setting the frequency of their change.

Accessing the User Sub-section

For accessing the *User* sub-section, go to Settings → Policies → User (Figure 11).

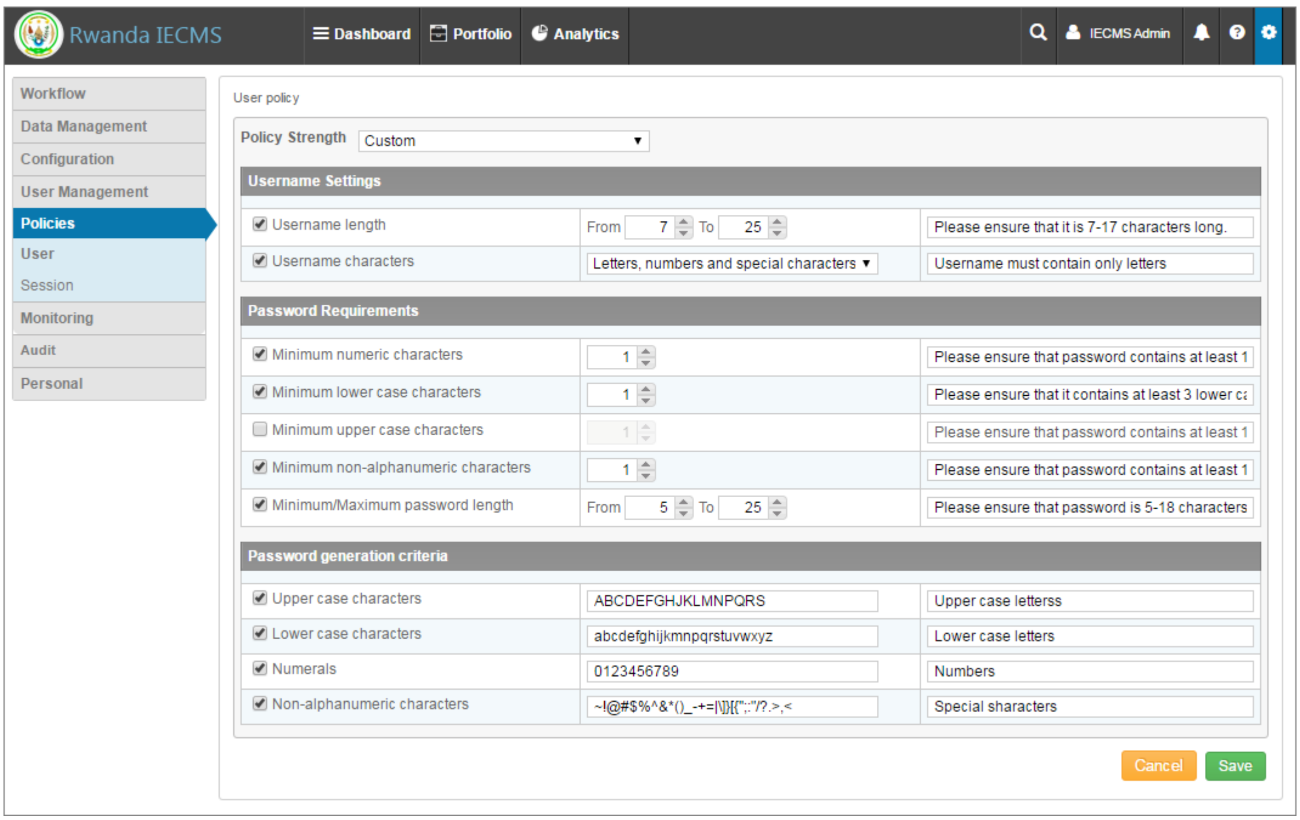

Figure 11: User Sub-section

Defining User Settings

In order to establish the naming principles and define the normal behavior for the username and password, follow the steps below:

1. Go to **Settings → Policies → User**...

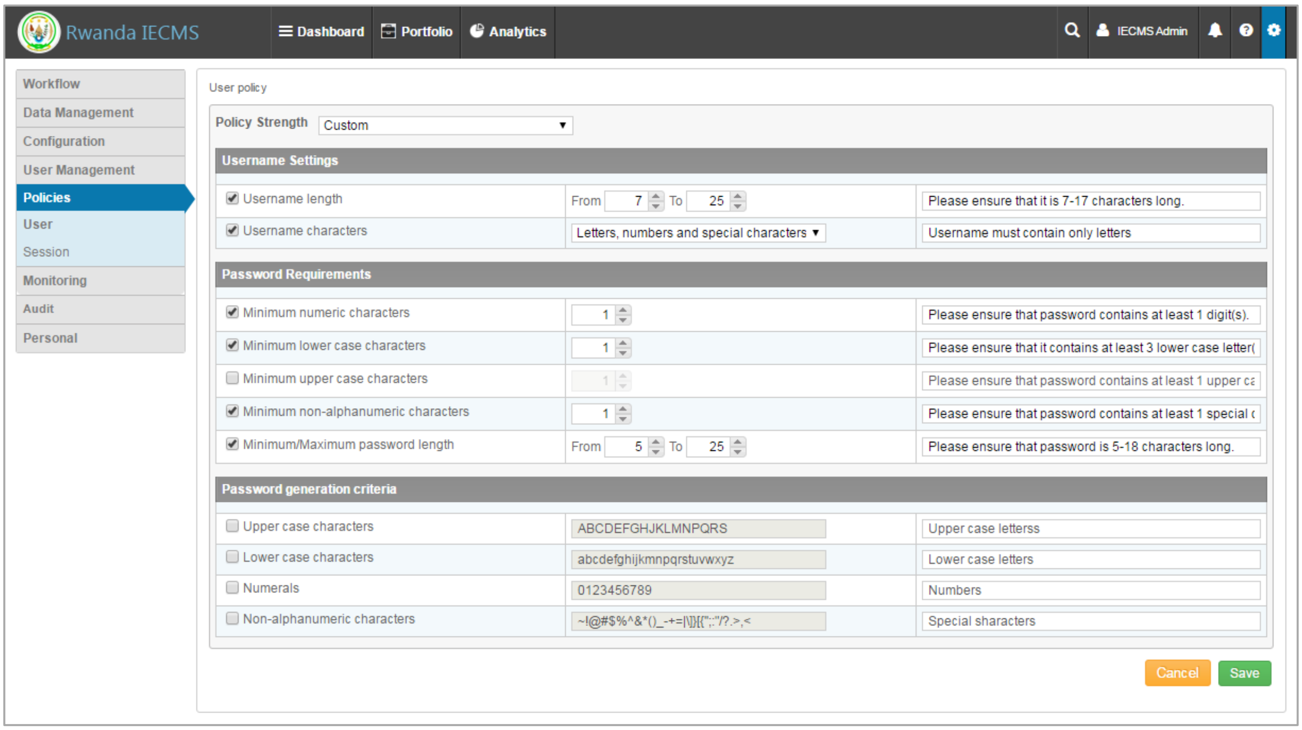

Figure 12: Defining User Settings

2. Select the **Policy Strength** from the drop-down list (Figure 12). The following options are available:
   - Low
   - Medium
   - High
   - Custom
3. Tick the checkbox to the left of the policy name to enable it and define its settings as described in the table below:

Component Name	Description
Username Settings	Indicate the minimal and maximal number of characters that a username must have. Also, specify the username composition, i.e. whether it can contain letters, numbers, and special characters. These settings will apply to all usernames created during the user registration process.
Password Requirements	Select the minimum allowed number of numeric, lower case, upper case and non-alphanumeric characters that a user password should contain. Also, specify the minimal and maximal number of characters that a password must have.
Password Generation Criteria	The password generation criteria will be used in the when the user forgets their password and requests a new one. Identify what upper and lower case letters as well as numerals and non-alphanumeric characters an automatically generated password must contain.

4. Provide additional comments or explanations for each policy.
5. Click the **Save** button to save the policy settings. Or, click **Cancel** to discard the modifications.

Managing Session

This chapter outlines how you can manage sessions. Sessions can be defined in terms of the period of time a user interfaces with an application. The user session begins when the user accesses the application and ends when the user quits the application.

For user session management purposes, it is very important to clearly state the conditions that a user session should meet for a successful and secure interaction with the application. These conditions may include setting the number of failed login attempts after which the user's account will be blocked, number of concurrent users per application, etc.

Accessing the Session Sub-section

For accessing the *Session* sub-section, go to Settings → Policies → Session (Figure 13).

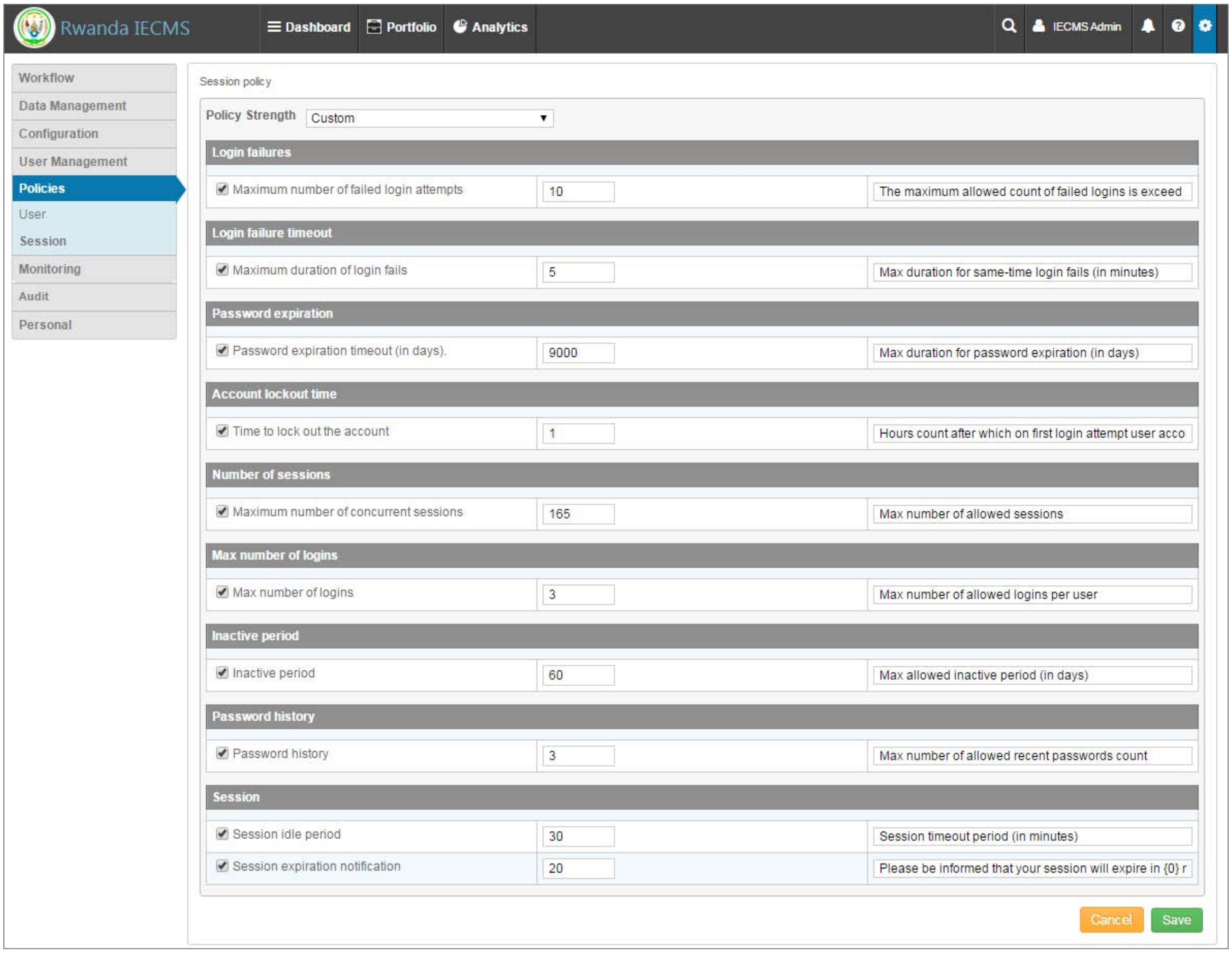

Figure 13: Session Sub-section

Defining Session Settings

In order to provide information on session governing policies, follow the steps below:

1. Go to **Settings → Policies → Session...**
2. Select the policy strength from the Policy Strength drop-down list (Figure 14). The following options are available:
   - Low
   - Medium
   - High
   - Custom
3. Tick the checkbox to the left of the policy name to enable it and define its settings as described in the table below:

Component Name	Description
Login failures	Specify the maximum number of unsuccessful attempts to log into the application that the user made.
Login failure timeout	Specify the allowed time frame (in minutes) during which the user should make the allowed number of unsuccessful attempts to log into the application before the user's account is blocked.
Password expiration	Identify the maximum amount of time (in days) after which the user is prompted to create a new password. Changing password after a defined number of days helps the system administrators to prevent passwords from being compromised.
Account lockout time	Indicate the amount of time (in hours) of lockout penalty that the user reaching the maximum allowed number of login failures should wait before their account is unblocked.
Number of sessions	Specify the maximum allowed number of users using the application within predefined period of time.
Max number of logins	Specify the maximum number of logins per user. If the user has reached the maximum number of allowed logins, login will be denied.
Inactive period	Specify the amount of time (in days) after which an inactive user account is disabled.
Password history	Enter the maximum number of recent passwords that the user is not allowed to reuse when prompted to change their passwords.
Session	Indicate the amount of time (in minutes) that a user session is allowed to stay idle before it is disconnected.

4. Provide additional comments or explanations for each policy.
5. Click the **Save** button to save the policy settings. Or, click **Cancel** to discard the modifications.

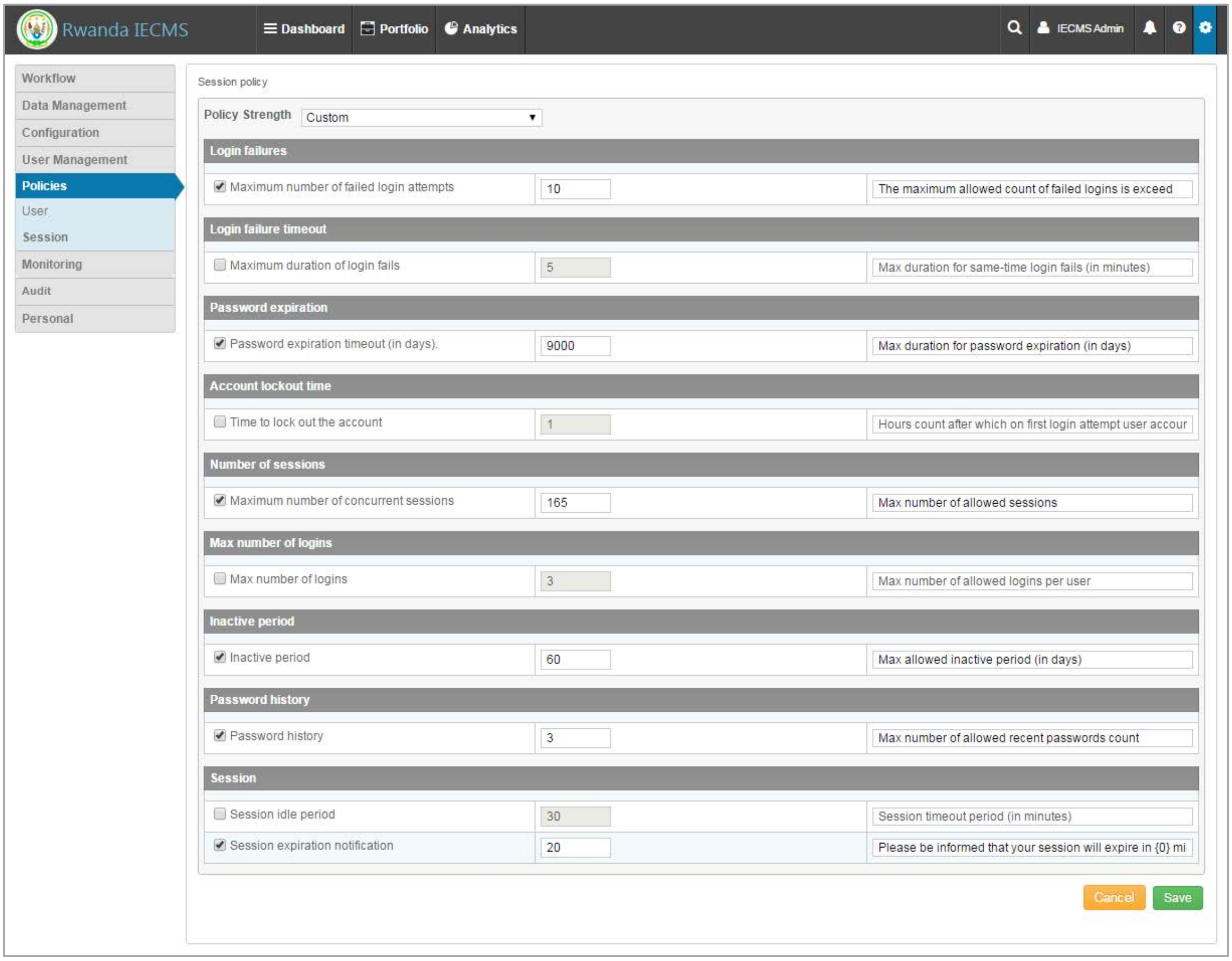

Figure 14: Defining Session Settings

MONITORING CONSOLE

This chapter describes the *Monitoring* console under the *Settings* section, where **Sessions** and **Locks** are managed.

Accessing the Monitoring Console

For accessing the *Monitoring* console, go to Settings → Monitoring (Figure 15).

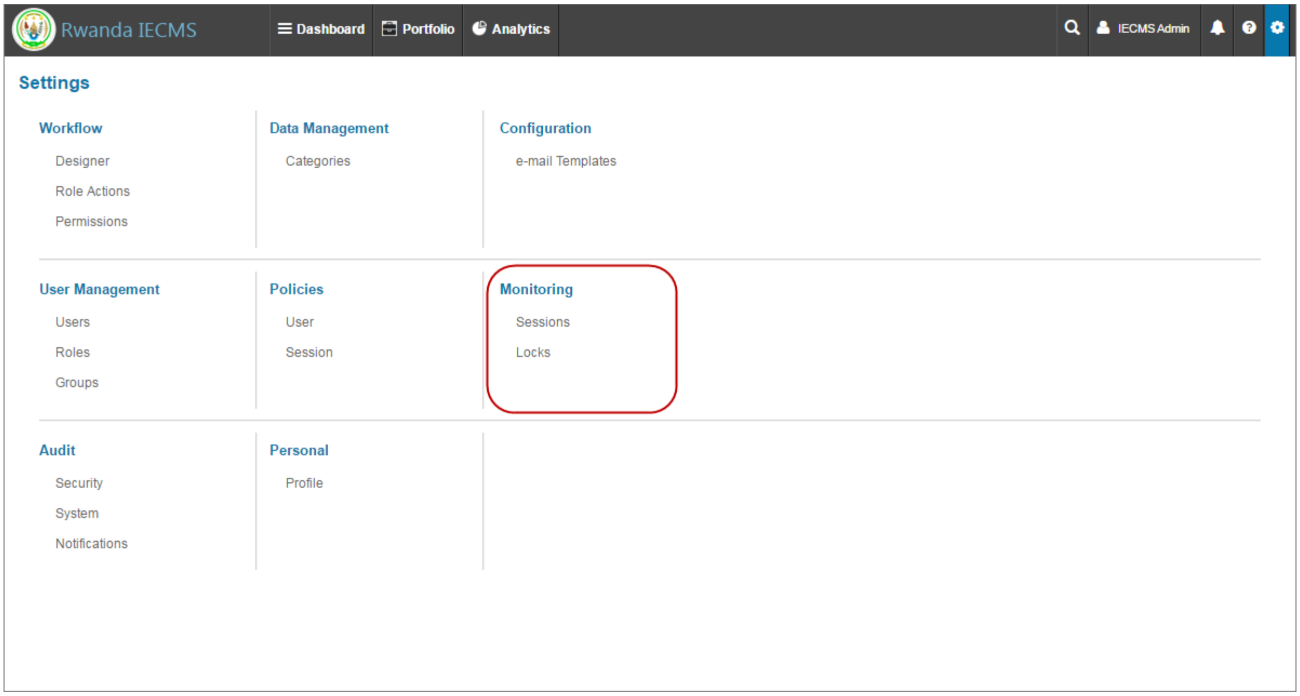

Figure 15: Monitoring Console

The *Monitoring* console consists of the following sub-sections:

- **Sessions** – to keep track of the user access to the application (see Managing Sessions);
- **Locks** – to manage locks (see Managing Locks).

Managing Sessions

The system offers a wide array of user administration options that allow the administrators to perform their duties in an easy and effective manner. One of these options includes the ability to monitor users' access to the application.

In order to monitor user sessions, go to Settings → Monitoring → Sessions (Figure 16). The user sessions will be organized into a table with the following columns:

Component Name	Description
ID	This is a unique number assigned to the session and used for referential purposes.
User	This shows the name of the user account that initiated the session.
IP	This indicates the IP address of the device the user used to access the application.
Browser	This displays the name of the browser used to access the application.
Date, Time (UTC)	This specifies the date and time when the user initiated the session.

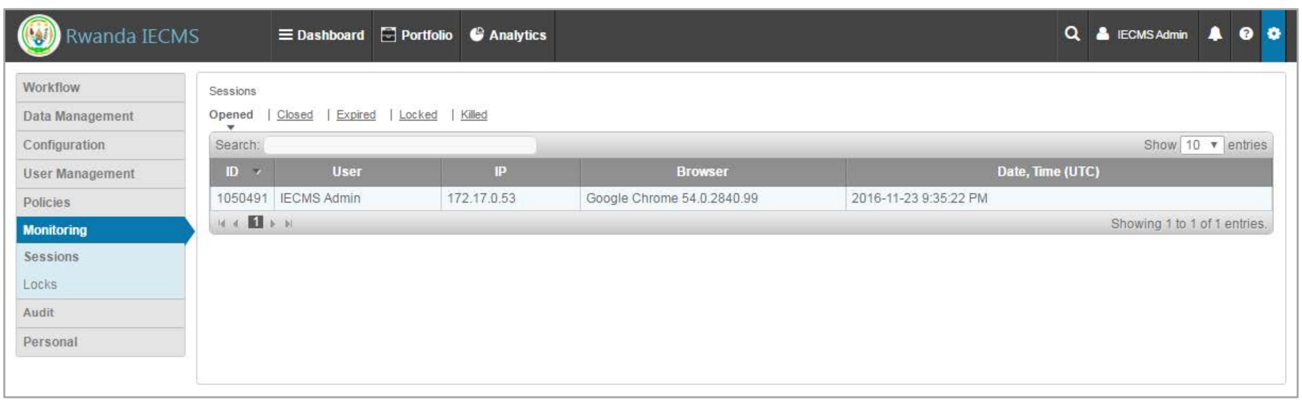

Figure 16: Monitoring Sessions

For your convenience, the user sessions are organized into separate tabs according to the session type. The available session types are as follows:

- Opened
- Closed
- Expired
- Locked
- Killed

To view the sessions of a definite type, click the respective link at the top of the *Sessions* table. All sessions matching the selection will display in the table.

Managing Locks

A lock is a mechanism for restricting user access to certain category elements. Locks are useful when the same category element can be accessed by several concurrent users. In this case, locking functionality ensures that these category elements are not simultaneously accessed by many users and only one user can modify it at a time.

The system is equipped with a comprehensive locking mechanism. Any time a user edits a shared category element, it acquires a lock and other users have to wait until the category element lock is released and it becomes available for editing again. The application collects and displays lock data. In order to manage lock data, go to Settings → Monitoring → Locks (Figure 17). The locked category items will be organized into a table with the following columns:

Component Name	Description
User	This shows the name of the user account that selected to modify the category element.
Category	This shows the name of the category that has a locked element.
Title	This displays the name of the locked category element.
Date, Time (UTC)	This specifies the date and time when the user initiated the session.
Unlock	This is used to hold the functionality for releasing the lock. For details see Unlocking a Category Element.

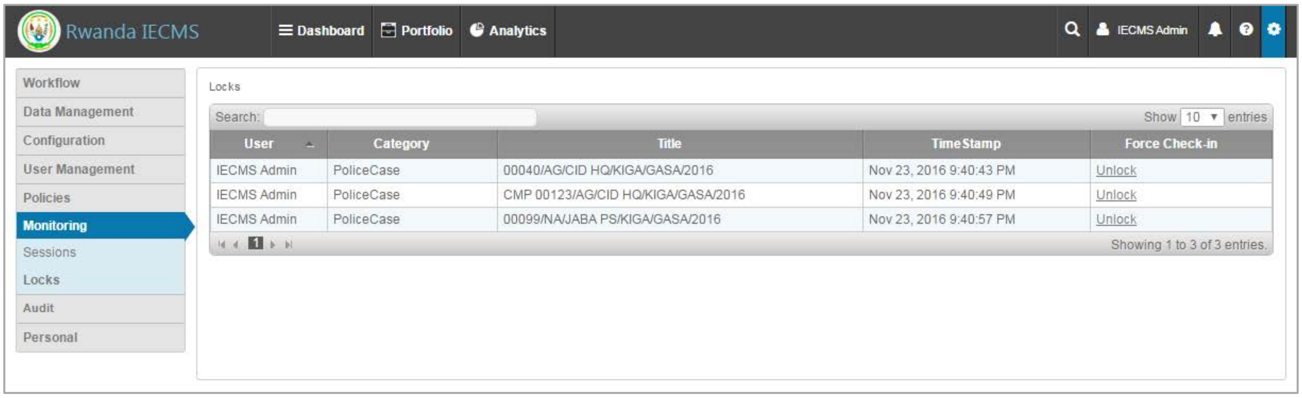

Figure 17: Monitoring Locks

Unlocking a Category Element

The administrator is allowed to unlock the locked elements if necessary.

In order to release a locked category element, follow the steps below:

1. Go to **Settings → Monitoring → Locks…**
2. Select the category item that needs to be unlocked and click the **Unlock** link in the far right side of the selected category element record. The element will become available for editing by other users.

Note: If the administrator releases a locked category element, the user working on it is notified about the change the next time a request is sent to the database, e.g. when the user navigates from one tab to another or selects to add an item. In this case, all unsaved information is lost.

AUDIT CONSOLE

This chapter describes the *Audit* section under the *Settings* section, where the application audit is performed.

Because *Rwanda IECMS* deals with sensitive passwords, it is important to have a complete record of all the operations performed using the application. All operations performed by the users including the password retrieval, account signup, etc. should be audited. The audit trails of the system are quite comprehensive providing information on 'who' performed 'what' operation and 'when'. *Rwanda IECMS* establishes strong accountability for all users and actions. All operations performed by users are audited with the timestamp and the source where the changes have been made.

Accessing the Audit Console

For accessing the *Audit* console, go to Settings → Audit (Figure 18).

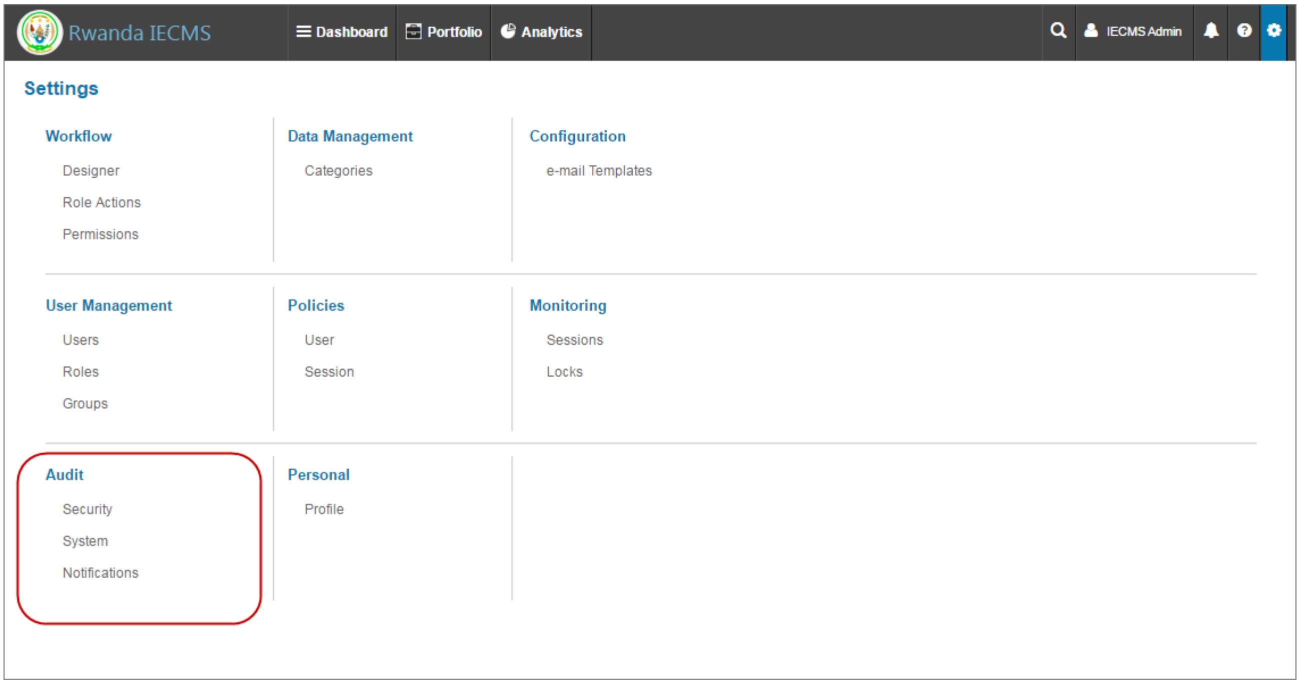

Figure 18: Audit Console

The *Audit* console consists of the following sub-sections:

- **Security** – to trail the records pertaining to the user's access to the application (see Managing Security);

- **System** – to trail the records pertaining to user management tasks (see Managing System);
- **Notifications** – to trail all notifications sent out using the application (see Managing Notifications).

Managing Security

This sub-section is used to record security-related information that can be used to re-establish a series of events, for example, unsuccessful login attempts, session termination, etc. To access the *Security* sub-section, go to Settings → Audit → Security (Figure 19).

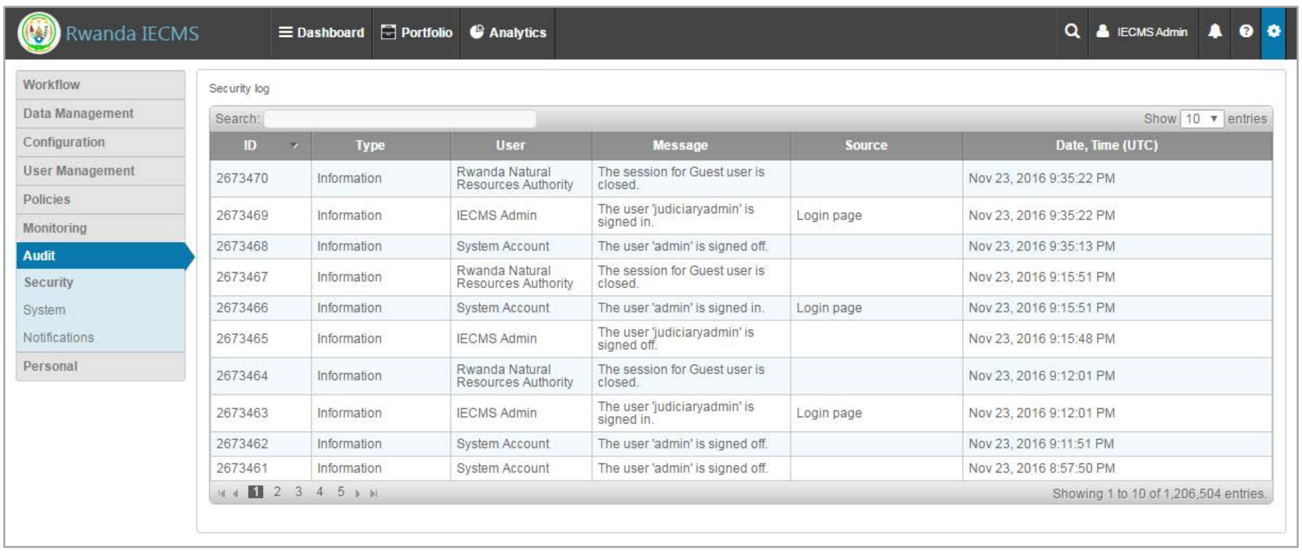

Figure 19: Performing Security Audit

The information displayed in the *Security* sub-section is organized in the form of a table with the following columns:

Component Name	Description
ID	This is an identification number assigned to the audit log item and used for referential purposes.
Type	This defines the log item type.
User	This identifies the user who performed the operation.

Message	This provides details on the action performed / error occurred.
Source	This identifies the application section where the action was performed / error occurred.
Date, Time (UTC)	This specifies the timestamp assigned to the action performed / error occurred.

Managing System

This sub-section is used to record user management related events to trail the operations that have been performed over users, their roles, and groups, for example, role creation, user modification, etc. To access the *System* sub-section, go to Settings → Audit → System (Figure 20).

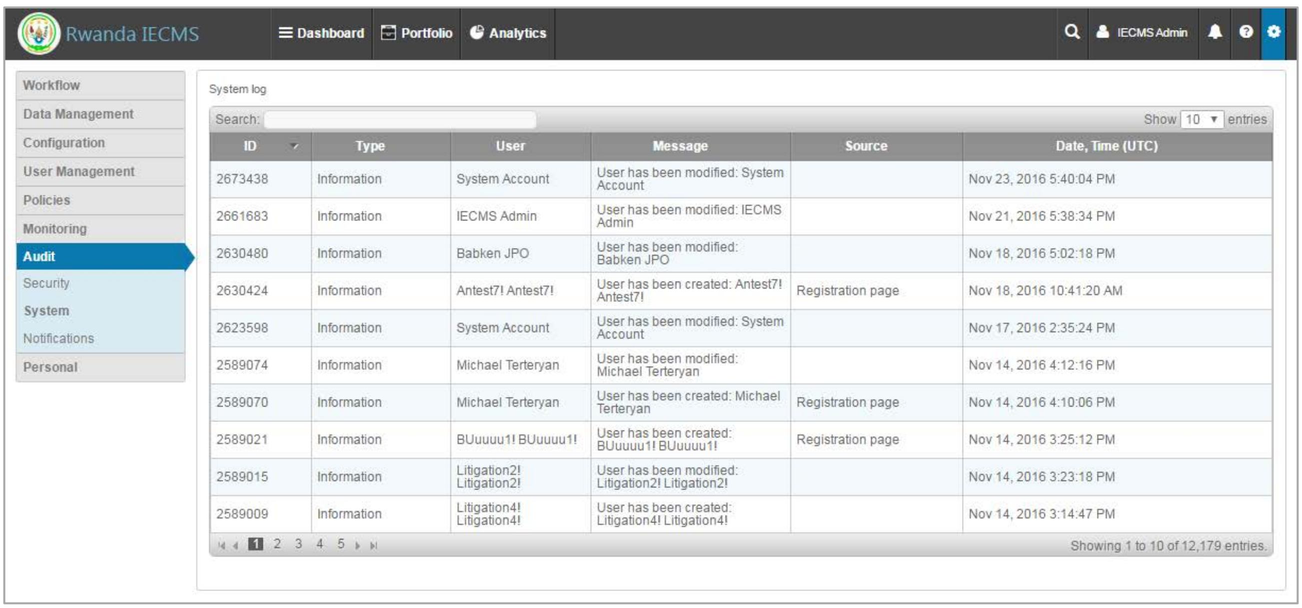

Figure 20: Performing System Audit

The information displayed in the *System* sub-section is organized in the form of a table having the following columns:

Component Name	Description
ID	This is an identification number assigned to the audit log item and used for referential purposes.
Type	This defines the log item type.
User	This identifies the user who performed the operation.
Message	This provides details on the action performed / error occurred.
Source	This identifies the application section where the action was performed / error occurred.
Date, Time (UTC)	This specifies the timestamp assigned to the action performed / error occurred.

Managing Notifications

This sub-section is used to track the e-mail notifications that have been sent out from the application on definite occasions such as user registration, uploading a file, deleting a file, etc. To access the *Notifications* sub-section, go to Settings → Audit → Notifications (Figure 21).

The information displayed in the *Notifications* sub-section is organized in the form of a table having the following columns:

Component Name	Description
ID	This is an identification number assigned to the audit log item and used for referential purposes.
Type	This defines the log item type.
User	This identifies the user who performed the operation.
Message	This provides details on the action performed / error occurred.

Source	This identifies the application section where the action was performed / error occurred.
Date, Time (UTC)	This specifies the timestamp assigned to the action performed / error occurred.

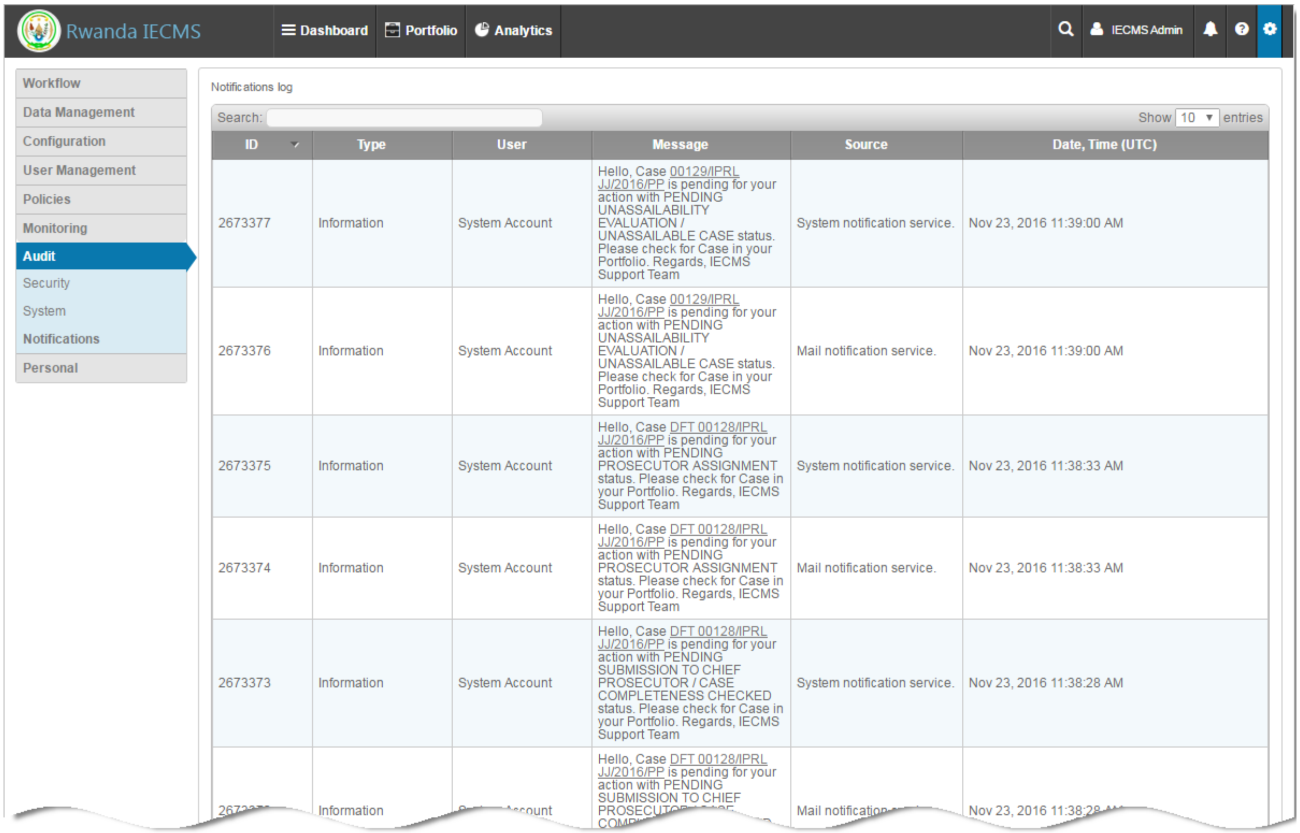

Figure 21: Performing Notifications Audit

PERSONAL CONSOLE

This chapter describes the *Personal* console under the *Settings* section, where the user's personal details and **Profile** information are managed.

Accessing the Personal Console

For accessing the *Personal* console, go to Settings → Personal or click the **My Profile** link from the username menu in the application header (Figure 22).

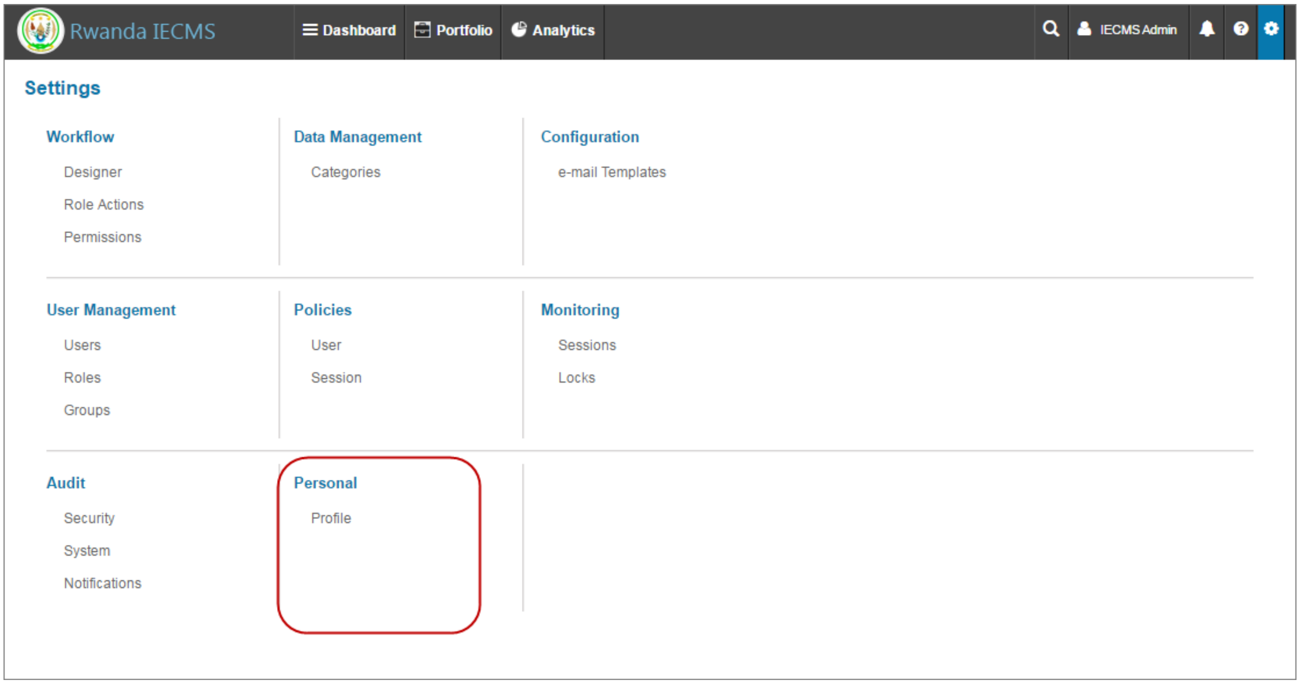

Figure 22: Personal Console

The *Personal* console consists of the following sub-section:

- **Profile** – to manage the user's personal details (see Managing Profile).

Managing Profile

This chapter outlines how you can manage personal information listed in the *Profile* section of the *Rwanda IECMS* application. More specifically, it describes how to enter or edit personal information.

Accessing the Profile Sub-section

The *Profile* sub-section can be accessed at Settings → Personal → Profile (Figure 22).

Once you access the *Profile* sub-section, you will be presented with your personal details form (Figure 23).

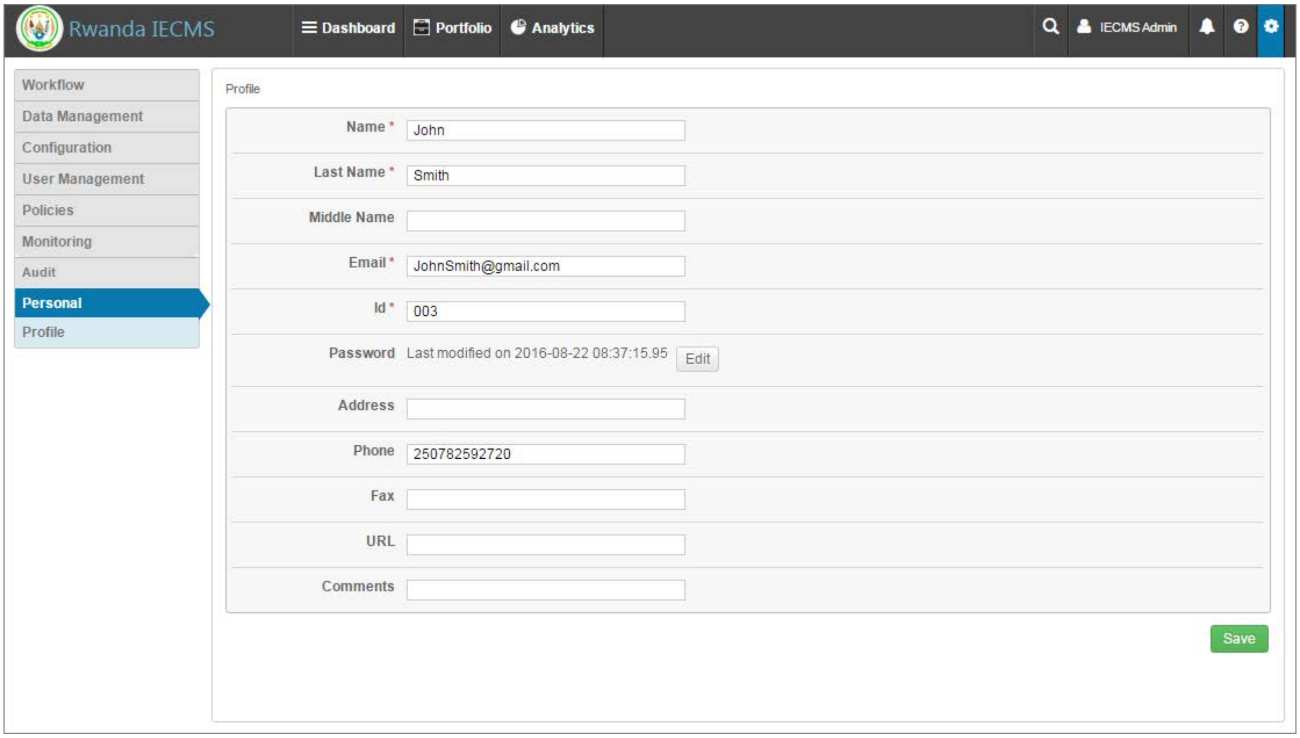

Figure 23: Profile Sub-section

The information displayed in this sub-section includes the following:

Component Name	Description
Name	This is the **Name** of the user provided when registering the user account.
Last Name	This is the **Last Name** of the user provided when registering the user account.

Middle Name	This is the **Middle Name** of the user provided when registering the user account.
Email	This is the **Email** address of the user.
Id	This is the **Id** number of the user.
Password	This is the **Password** of the user account.
Phone	This is the **Phone** number of the user.
Fax	This is the **Fax** number of the user.
URL	This is the user's web address.
Comments	Any relevant **Comments** should be provided here.

LOGGING OUT

Once you have finished using the *Rwanda IECMS* application, it is necessary to log out. To log out from the application, click your account name in the upper right corner of the application window and then click the **Logout** link.

REFERENCES

Please, refer to the following Rwanda IECMS related documents to obtain more information about the system and how it functions:

- Rwanda IECMS Analytical Interface User Manual
- Rwanda IECMS Portfolio User Manual
- Rwanda IECMS Dashboard User Manual
- Rwanda IECMS Rwanda National Police Application User Manual
- Rwanda IECMS Rwanda National Public Prosecution Authority Application User Manual
- Rwanda IECMS Rwanda Judiciary Application User Manual
- Rwanda IECMS Rwanda Correctional Service Application User Manual
- Rwanda IECMS Civil Litigation Service Application User Manual
- Rwanda IECMS Task Form User Manual
- Rwanda IECMS Legal Entity Form User Manual
- Rwanda IECMS Individual Form User Manual
- Rwanda IECMS Case Processing Workflow User Manual
- Rwanda IECMS User Management Administrator's Guide
- Rwanda IECMS Data Management Administrator's Guide
- Rwanda IECMS Workflow Management Administrator's Guide

APPENDIX I: E-MAIL TEMPLATE PARAMETERS

The table below describes the parameters that different e-mail template bodies can have.

Template Name	Description
New Account Registration	Dear <username>, This is automatic e-mail, please do not reply. Your account has been successfully created. Your login: <login> Please click to link below to confirm your e-mail address and account <confirmation-url>. Regards, IECMS
Password has been recovered	Dear <username>, This is automatic e-mail, please do not reply. Your password has been successfully recovered. Your new password is: <password> Regards, IECMS Support Team
System is under maintenance	Dear Administrator, This is automatic e-mail, please do not reply. The system is under maintenance mode. Regards, IECMS Support Team

System is out from maintenance	Dear Administrator, This is automatic e-mail, please do not reply. The system is out from maintenance mode. Regards, IECMS Support Team
The password has been changed	Dear <username>, This is automatic e-mail, please do not reply. Your password has been successfully changed. Regards, IECMS Support Team
Case is pending for your action	Hello, Case <CaseNumberStr> is pending for your action with <WFState> status. Please check for Case in your Portfolio. Regards, IECMS
Task is in Pending state	Hello, Task <TaskID> is in Pending state. Regards, IECMS Support Team
Task has been Cancelled	Hello, Task <TaskID> has been Cancelled. Regards, IECMS Support Team
Task has been Completed	Hello, Task <TaskID> has been Completed. Regards, IECMS Support Team
New task is assigned to you	Hello,

	New Task <TaskID> has been assigned to you. Regards, IECMS Support Team