Smarter Balanced Assessment Consortium:

Monitoring and Alerting User Guide

2014–2015

Published September 30, 2014

Table of Contents

Table of Figures

INTRODUCTION TO THIS USER GUIDE

This user guide supports individuals using the Monitoring and Alerting System to monitor and maintain the components or applications that are deployed for a tenant. This introduction describes the contents of this document and includes a key for identifying icons and elements.

This user guide provides information about the Monitoring and Alerting System in a series of three sections, as follows:

- Section I, Overview of the Monitoring and Alerting System, provides an overview of the system and the user roles for accessing the system.
- Section II, Getting Started with the Monitoring and Alerting System, explains how to log in to the Monitoring and Alerting System and describes the overall layout of the Monitoring and Alerting System Interface.
- Section III, Performing Monitoring and Alerting Tasks, describes how to perform different monitoring tasks in the Monitoring and Alerting System.

Table 1. Key Icons and Elements

Icon	Description
⚠	**Warning**: This symbol appears with text that contains extremely important information regarding actions that may cause errors.
⚠	**Caution**: This symbol appears with text that contains important information regarding a task.
🗒	**Note**: This symbol appears next to text that contains helpful information or reminders.
1. text 2. text	Text that appears in gray boxes provides instructions relevant to the task described. • Numbered (ordered) lists provide step-by-step instructions. • Bulleted lists provide instructions that do not need to be done in a specific order.
[**Text**]	Text in brackets is used to indicate a link or button that is clickable.
Text	Text in italics indicates field names or labels.
"Text"	Text in quotation marks indicates the value specified for a field.

SECTION I. OVERVIEW OF THE MONITORING AND ALERTING SYSTEM

The Monitoring and Alerting System is a web-based system and is one of the core applications that must be deployed with any other component used by the tenant at any given deployment level. It acts as a centralized repository for all the logs and alerts generated by the components deployed for a tenant.

This system serves as a powerful tool that can be used by system administrators to monitor the health of all the components that are deployed for a tenant. It allows administrators to view the logs and alerts generated by a running application and thereby monitor any errors, warnings, or debugging information generated during a program’s execution. It also allows administrators to create notification rules and groups of members or personnel to whom automatic notification emails can be sent in case the notification rules are met.

User Roles and Access

The Monitoring and Alerting System is a core infrastructural application and is accessible to only a limited number of users. Currently only users with the Administrator user role can view and access the Monitoring and Alerting System.

SECTION II. GETTING STARTED WITH THE MONITORING AND ALERTING SYSTEM

This section provides information about getting started with the Monitoring and Alerting System:

- Logging in to the Monitoring and Alerting System
- Understanding the Monitoring and Alerting System layout

Logging in to the Monitoring and Alerting System

To access the Monitoring and Alerting System, you must have an authorized user name and password. Your system administrator will be responsible for setting up your user account and providing you with the login credentials.

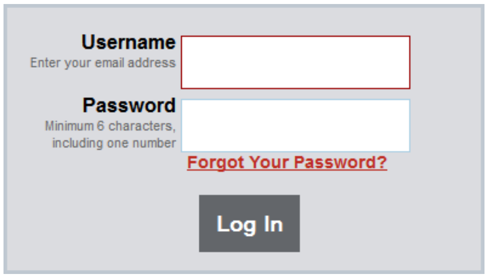
The Monitoring and Alerting System uses the Single Sign On (SSO) System, which is responsible for user authentication and authorization and allows you to log in to the Smarter Balanced systems. After logging in, you can switch between systems without having to log in and out of each system.

To log in to the Monitoring and Alerting System:

1. Open your web browser and navigate to the Monitoring and Alerting System using the URL provided to you.

   You will be directed to the Single Sign On Login screen shown in Figure 1.
2. In the *Username* field, enter your user name.
3. In the *Password* field, enter your password.
4. Click the [Log In] button. You will be directed to the Monitoring and Alerting System home screen, provided your login is authenticated.

Figure 1. Login Screen

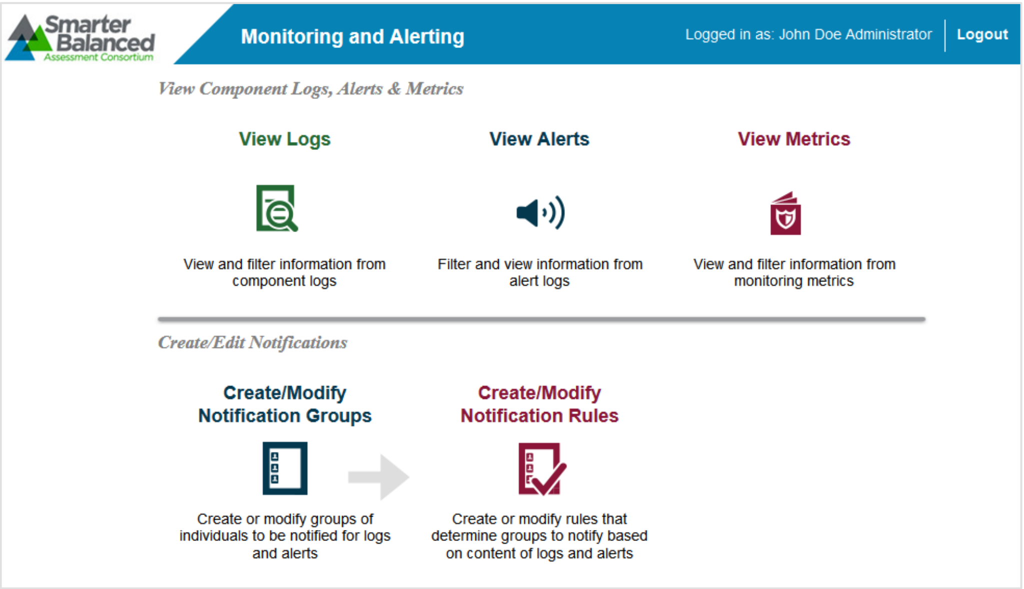


Understanding the Monitoring and Alerting System Layout

You can access the different features of the Program Management System from the home screen (see Figure 2) that appears when you first log in to the system.

Use the on-screen tools and buttons to navigate within the system. Do not use your web browser's back button.

Figure 2. Monitoring and Alerting System Home Screen



Monitoring and Alerting

Logged in as: John Doe Administrator | Logout

View Component Logs, Alerts & Metrics

View Logs

View and filter information from component logs

View Alerts

Filter and view information from alert logs

View Metrics

View and filter information from monitoring metrics

Create/Edit Notifications

Create/Modify Notification Groups

Create or modify groups of individuals to be notified for logs and alerts

Create/Modify Notification Rules

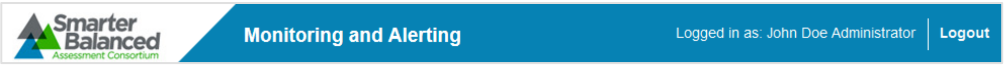
Create or modify rules that determine groups to notify based on content of logs and alerts

The Monitoring and Alerting System layout includes the features described below.

Header

The header that appears on every screen provides information about the user logged in to the system and includes tools and buttons to perform different tasks, as shown in Figure 3.

Figure 3. Header



Monitoring and Alerting

Logged in as: John Doe Administrator | Logout

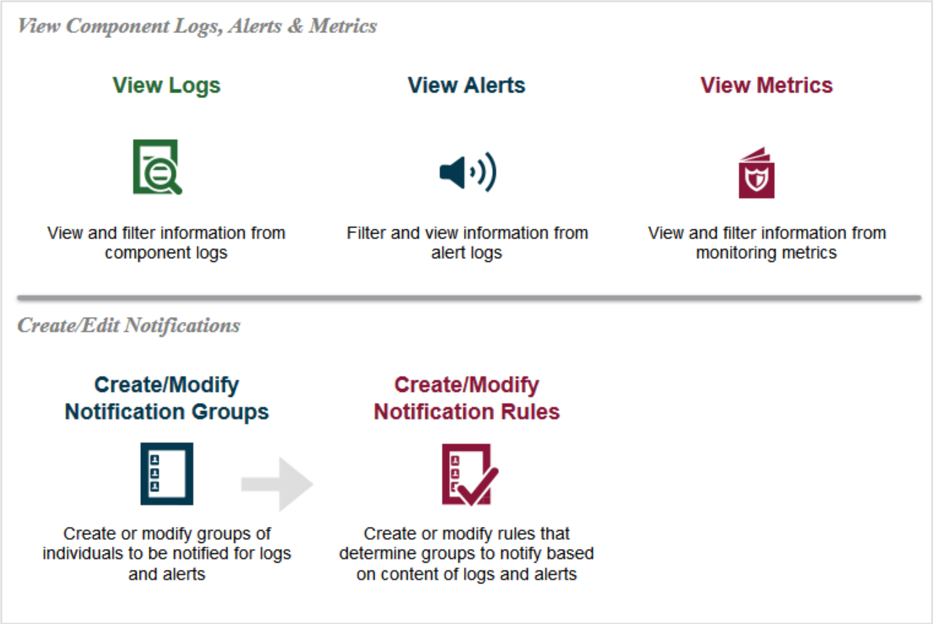
The header has the following features:

- User Identification: When you log in to the system, your name and user role are displayed on the header.
- [**Logo**]: The Smarter Balanced Assessment Consortium logo acts as a button that brings you back to the home screen.
- [**Logout**]: This button enables you to log out of the system.

Task Icons

The different monitoring and alerting tasks are displayed as icons on the home screen. Each task icon acts as a link that takes you to the specified task screen.

Figure 4. Monitoring and Alerting Task Icons



View Component Logs, Alerts & Metrics

View Logs

View and filter information from component logs

View Alerts

Filter and view information from alert logs

View Metrics

View and filter information from monitoring metrics

Create/Edit Notifications

Create/Modify Notification Groups

Create or modify groups of individuals to be notified for logs and alerts

Create/Modify Notification Rules

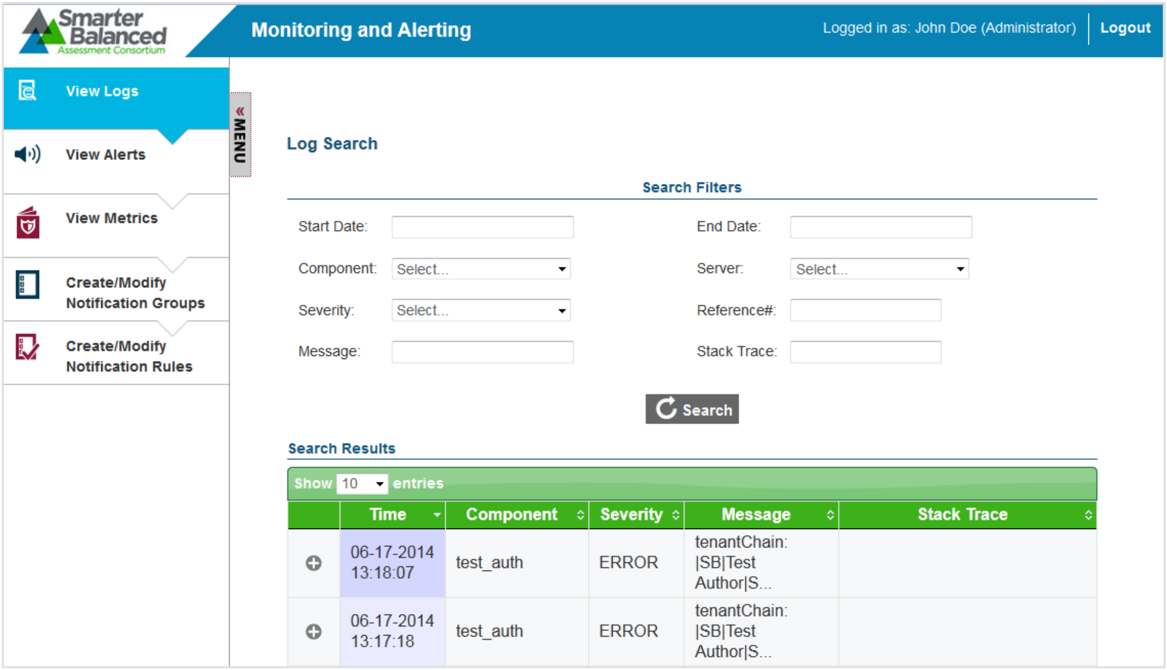
Create or modify rules that determine groups to notify based on content of logs and alerts

When you select a task, a menu is displayed on the screen. You can navigate through the different tasks using the menu. To return to the home screen and view the task icons, click the logo on the header.

Task Screens

The Monitoring and Alerting System uses only one screen layout, which is the search screen. When you first access a task, you are taken to the task's search screen by default. Figure 5 shows a sample search screen.

Figure 5. Sample Search Screen



	Time	Component	Severity	Message	Stack Trace
⊕	06-17-2014 13:18:07	test_auth	ERROR	tenantChain: |SB|Test Author|S...	
⊕	06-17-2014 13:17:18	test_auth	ERROR	tenantChain: |SB|Test Author|S...	

The search screen consists of the following two sections:

- Search Filters Section: This section allows you to search for records that have been created for the selected task. It consists of
  - search criteria fields applicable to the task that you are viewing, where you can specify the required search criteria; and
  - a [Search] button that enables you to search for records based on the specified criteria; and

The Search Filters section may also consist of a [New] button that opens a popup window from which you can create a new record. However, the button is not available for all task categories.

- Table of Records Section: The table of records displays the records that have been created for the selected task based on the search filter specifications. You can search for and filter the records using the search filters. The table consists of the following features:
  - You can sort the data displayed in the columns by clicking the column header. Not all columns can be sorted. If a column can be sorted, arrows will be displayed on the column header.
  - A navigation panel is displayed at the bottom of the table that enables you to navigate through the retrieved records. It also displays the number of records that matched the specified search criteria.

SECTION III. PERFORMING MONITORING AND ALERTING TASKS

The core functionality of the Monitoring and Alerting System is to allow system administrators to view and monitor logging information for components deployed for a tenant.

The different monitoring and alerting tasks include the following:

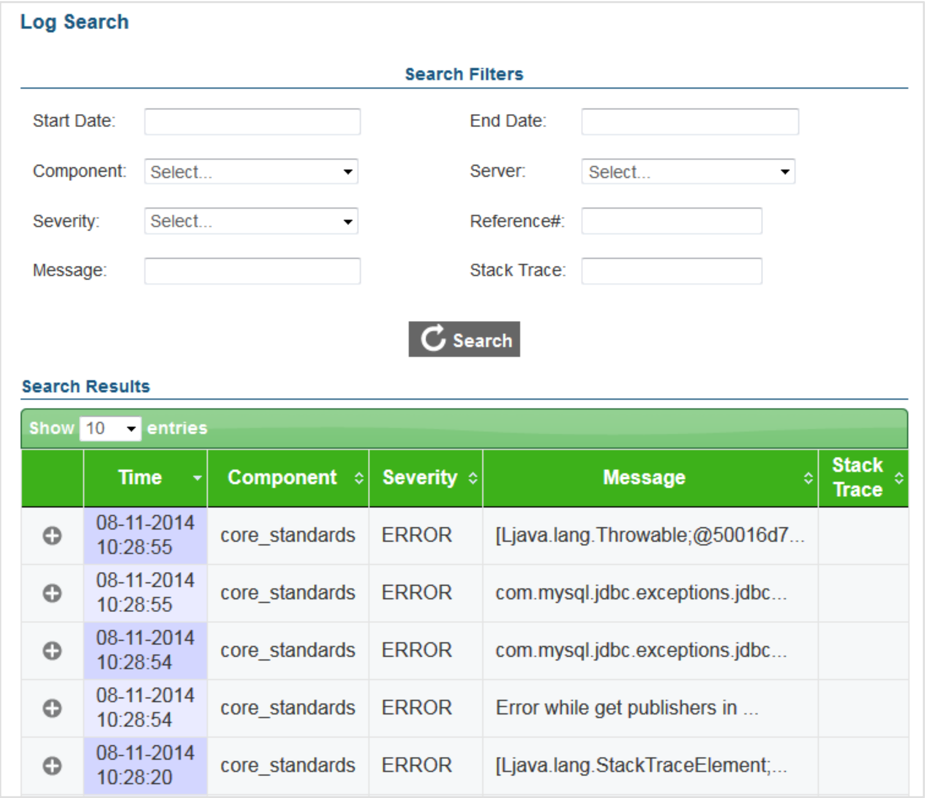
- Viewing Logs
- Viewing Alerts
- Viewing Metrics
- Managing Notification Groups
- Managing Notification Rules

Viewing Logs

The Monitoring and Alerting System allows you to view the logs generated for deployed components. A log is a routinely generated file that can list all the actions that have occurred for a component. You can enable or disable logging for a component based on the type of event that is being logged. For example, to reduce the large volume of logs, you may choose to only enable logging for events that generate an error or warning.

From the ***Log Search*** screen (see Figure 6), authorized users can search for and view component logs.

Figure 6. Log Search Screen



Log Search

Search Filters

Start Date:		End Date:	
Component:	Select...	Server:	Select...
Severity:	Select...	Reference#:	
Message:		Stack Trace:	

Search

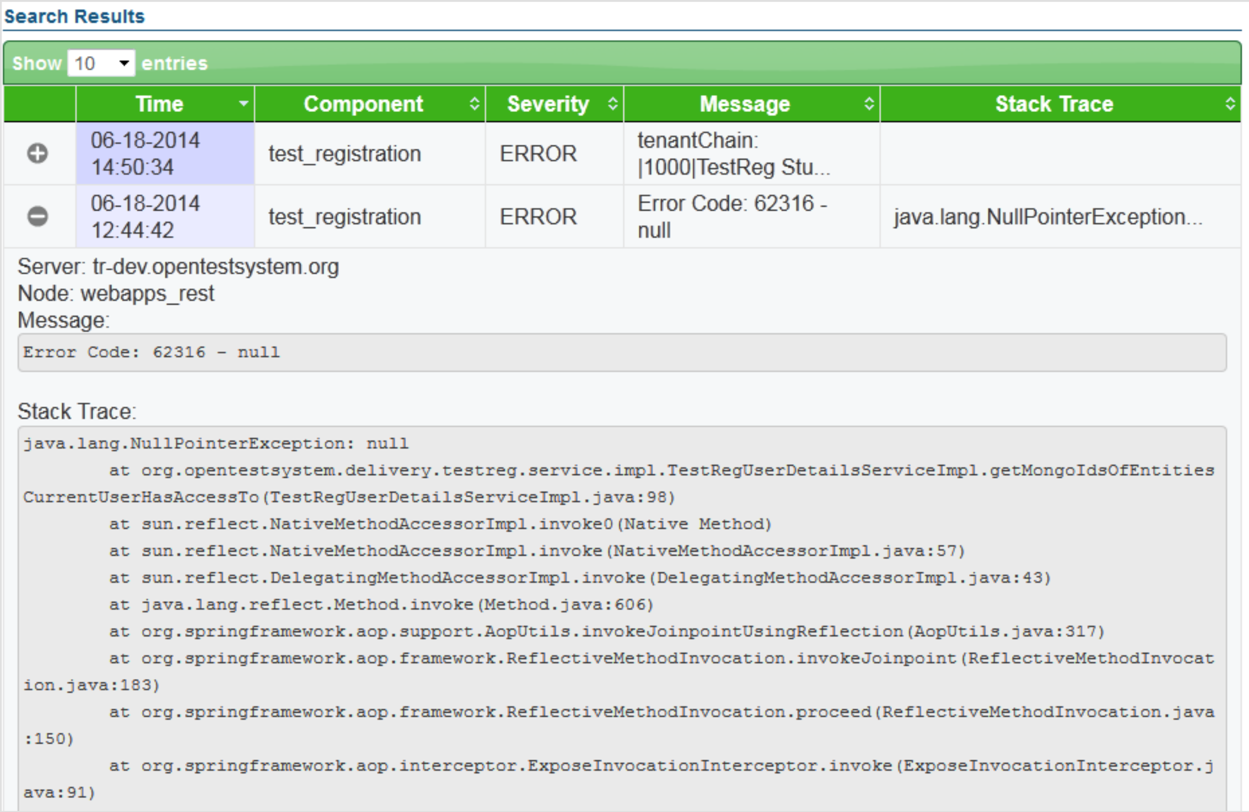
Search Results

Show 10 entries

	Time	Component	Severity	Message	Stack Trace
⊕	08-11-2014 10:28:55	core_standards	ERROR	[Ljava.lang.Throwable;@50016d7...	
⊕	08-11-2014 10:28:55	core_standards	ERROR	com.mysql.jdbc.exceptions.jdbc...	
⊕	08-11-2014 10:28:54	core_standards	ERROR	com.mysql.jdbc.exceptions.jdbc...	
⊕	08-11-2014 10:28:54	core_standards	ERROR	Error while get publishers in ...	
⊕	08-11-2014 10:28:20	core_standards	ERROR	[Ljava.lang.StackTraceElement;...	

To search for component logs:

1. On the home screen (see Figure 2), click the View Logs icon. The ***Log Search*** screen appears listing all the existing logs for the deployed components.
2. Enter any search criteria you want to include using the available search filters. The different search filters are described in Figure 7. Sample Component Log Details



Search Results

Show 10 entries

	Time	Component	Severity	Message	Stack Trace
⊕	06-18-2014 14:50:34	test_registration	ERROR	tenantChain: |1000|TestReg Stu...	
⊖	06-18-2014 12:44:42	test_registration	ERROR	Error Code: 62316 - null	java.lang.NullPointerException...

Server: tr-dev.opentestsystem.org
Node: webapps_rest
Message:

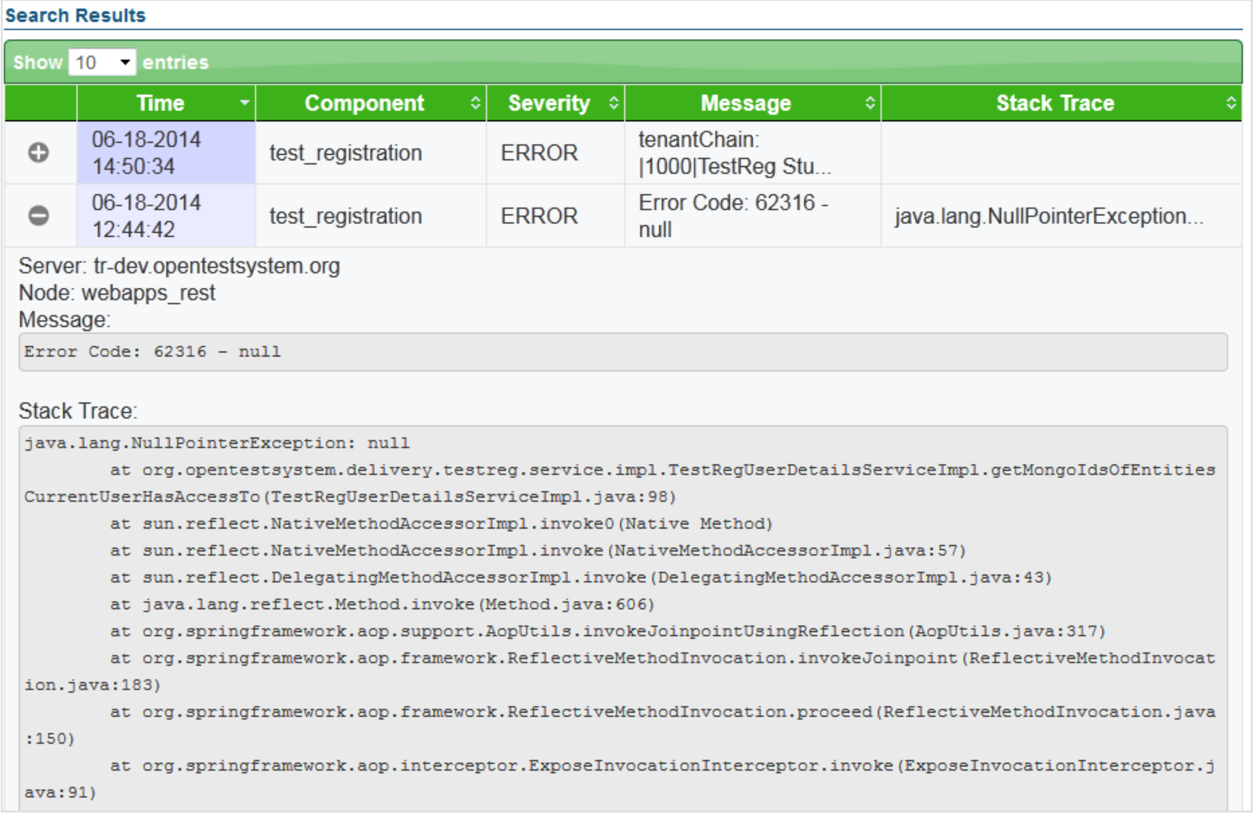
```
Error Code: 62316 - null
```

Stack Trace:

```
java.lang.NullPointerException: null
        at org.opentestsystem.delivery.testreg.service.impl.TestRegUserDetailsServiceImpl.getMongoIdsOfEntities
CurrentUserHasAccessTo(TestRegUserDetailsServiceImpl.java:98)
        at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
        at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:57)
        at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
        at java.lang.reflect.Method.invoke(Method.java:606)
        at org.springframework.aop.support.AopUtils.invokeJoinpointUsingReflection(AopUtils.java:317)
        at org.springframework.aop.framework.ReflectiveMethodInvocation.invokeJoinpoint(ReflectiveMethodInvocat
ion.java:183)
        at org.springframework.aop.framework.ReflectiveMethodInvocation.proceed(ReflectiveMethodInvocation.java
:150)
        at org.springframework.aop.interceptor.ExposeInvocationInterceptor.invoke(ExposeInvocationInterceptor.j
ava:91)
```

3. Table 2.
4. Click the [**Search**] button. The screen will display the search results table containing the logs that match the search criteria.
5. To view the log details, click the expand [⊕] button next to the required log. A sample log detail is shown in Figure 7.

Figure 7. Sample Component Log Details



	Time	Component	Severity	Message	Stack Trace
⊕	06-18-2014 14:50:34	test_registration	ERROR	tenantChain: |1000|TestReg Stu...	
⊖	06-18-2014 12:44:42	test_registration	ERROR	Error Code: 62316 - null	java.lang.NullPointerException...

Server: tr-dev.opentestsystem.org
Node: webapps_rest
Message:

```
Error Code: 62316 - null
```

Stack Trace:

```
java.lang.NullPointerException: null
        at org.opentestsystem.delivery.testreg.service.impl.TestRegUserDetailsServiceImpl.getMongoIdsOfEntities
CurrentUserHasAccessTo(TestRegUserDetailsServiceImpl.java:98)
        at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
        at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:57)
        at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
        at java.lang.reflect.Method.invoke(Method.java:606)
        at org.springframework.aop.support.AopUtils.invokeJoinpointUsingReflection(AopUtils.java:317)
        at org.springframework.aop.framework.ReflectiveMethodInvocation.invokeJoinpoint(ReflectiveMethodInvocat
ion.java:183)
        at org.springframework.aop.framework.ReflectiveMethodInvocation.proceed(ReflectiveMethodInvocation.java
:150)
        at org.springframework.aop.interceptor.ExposeInvocationInterceptor.invoke(ExposeInvocationInterceptor.j
ava:91)
```

Table 2: Log Search Screen Search Filters

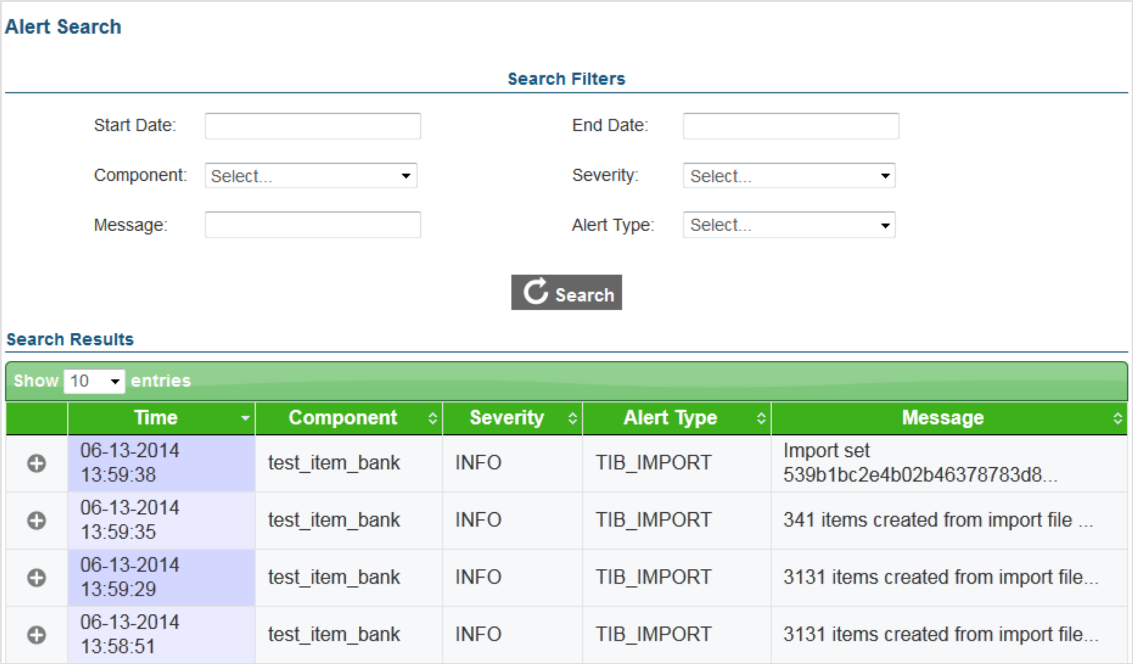
Search Filter	Description
Start Date	Refers to the date when the log was started. You can select the specific date from the calendar that is displayed when you place your cursor in the text box.
End Date	Refers to the date when the log ended. You can select the specific date from the calendar that is displayed when you place your cursor in the text box.
Component	Refers to the component to which the log belongs. You can select the component from the drop-down list that displays the names of all the components for which logs have been generated.
Server	Refers to the server on which the component is installed. You can select the server name from the drop-down list that is a dynamic list containing the names of the servers associated with existing logs.
Severity	Refers to the type of event or information captured in the log entry. You can select the required type from the drop-down list that contains the following options: • Error: Indicates a significant problem, such as a loss of functionality or data. • Warn: Indicates a problem that is not immediately significant but that may cause future complications. For example, an application can log a warning event if disk space is low. • Info: Indicates a significant successful operation. • Debug: Indicates troubleshooting information used for resolving software problems. • Trace: Indicates logging information about a program’s execution that is typically used for debugging and diagnosing software problems.
Reference#	Refers to the error code that may be displayed in the event message. All logged events may not contain a reference number or error code.
Message	Refers to the event message. You can search for events by the complete or partial message.
Stack Trace	Refers to the list of the methods that an application was calling at the time of the logged event. You can search by the exception listed at the top of the stack. Some examples of exceptions are java.lang.NullPointer and java.lang.RuntimeException.

Viewing Alerts

The Monitoring and Alerting System allows you to view alerts generated by deployed components. Each component has inbuilt alerts that are triggered by specific discrete events. You can be notified whenever an alert event occurs and thereby ensure the smooth running of the component. Not all alerts indicate problems or issues with the functioning of the component. Alerts can also be informational.

From the ***Alert Search*** screen (see Figure 8), authorized users can search for and view component alerts.

Figure 8. Alert Search Screen



Alert Search

Search Filters

Start Date:		End Date:	
Component:	Select...	Severity:	Select...
Message:		Alert Type:	Select...

Search Results

	Time	Component	Severity	Alert Type	Message
⊕	06-13-2014 13:59:38	test_item_bank	INFO	TIB_IMPORT	Import set 539b1bc2e4b02b46378783d8...
⊕	06-13-2014 13:59:35	test_item_bank	INFO	TIB_IMPORT	341 items created from import file ...
⊕	06-13-2014 13:59:29	test_item_bank	INFO	TIB_IMPORT	3131 items created from import file...
⊕	06-13-2014 13:58:51	test_item_bank	INFO	TIB_IMPORT	3131 items created from import file...

To search for component alerts:

1. On the home screen (see Figure 2), click the View Alerts icon. Alternatively, select the View Alerts option from the menu. The ***Alerts Search*** screen appears listing all the existing alerts for the deployed components.
2. Enter any search criteria you want to include using the available search filters. The different search filters are described in
3. Table 3.
4. Click the [**Search**] button. The screen will display the search results table containing the alerts that match the search criteria.
5. To view the alert details, click the expand [⊕] button next to the required alert.

Table 3: Alert Search Screen Search Filters

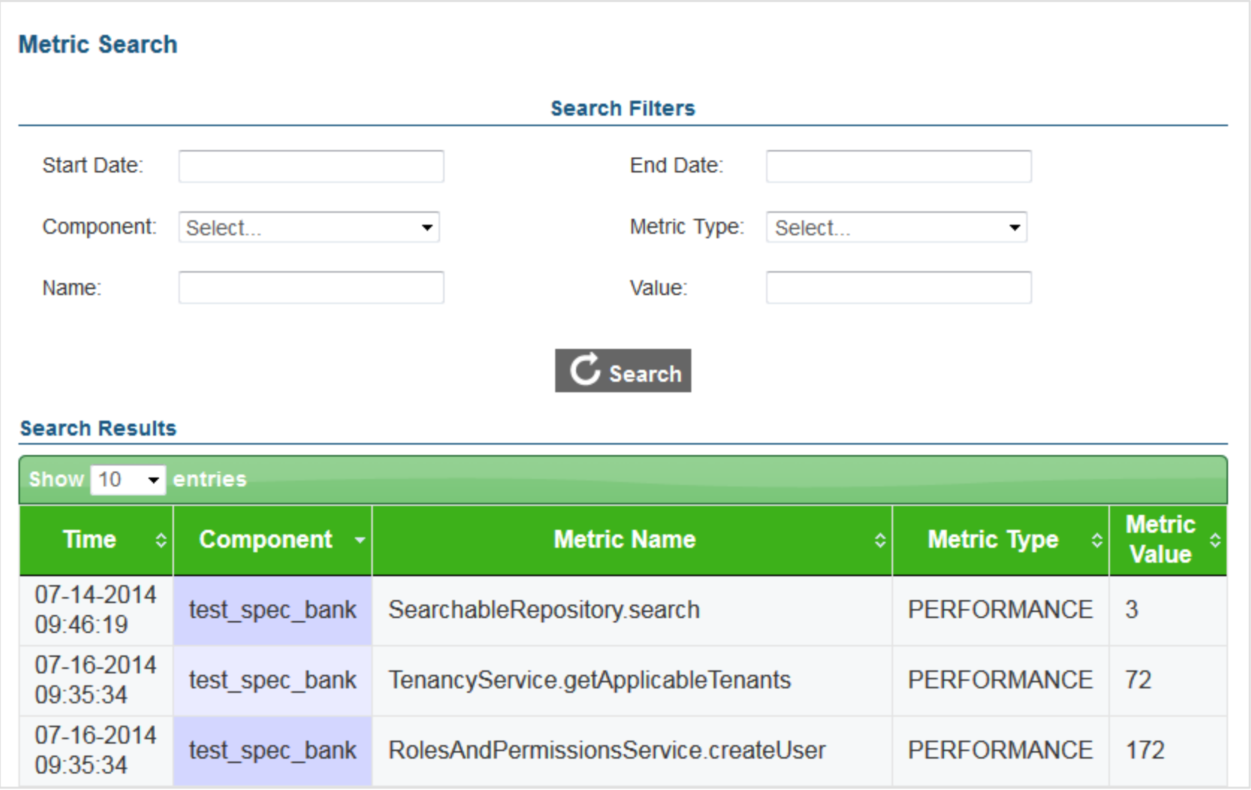
Search Filter	Description
Start Date	Refers to the date when the alert was created. You can select the required date from the calendar that is displayed when you place your cursor in the text box.
End Date	Refers to the date when the alert ended. You can select the required date from the calendar that is displayed when you place your cursor in the text box.
Component	Refers to the component for which the alert was generated. You can select the component from the drop-down list that displays the names of all the components for which alerts have been generated.
Severity	Refers to the type of event or information captured in the alert entry. You can select the required type from the drop-down list. The available options are: • Error: Indicates a significant problem, such as inability to perform an action. • Warn: Indicates a problem that is not immediately significant but that may cause future complications. • Info: Indicates a significant successful operation. • Debug: Indicates troubleshooting information used for resolving software problems. • Trace: Indicates logging information about a program's execution that is typically used for debugging and diagnosing software problems.
Message	Refers to the alert message. You can search for alerts by the complete or partial message.
Alert Type	Refers to the component-specific alert name. You can select the specific type from the drop-down list that is a dynamic list containing all the alert types that have been generated. If an alert has not been generated for an alert type, the alert type will not be listed in the drop-down list.

Viewing Metrics

The Monitoring and Alerting System also allows you to view different types of metrics for the components deployed for a tenant. Each component has inbuilt metrics that are used to measure different aspects of a component's performance.

From the ***Metric Search*** screen (see Figure 9), authorized users can search for and view component metrics.

Figure 9. Metric Search Screen



Time	Component	Metric Name	Metric Type	Metric Value
07-14-2014 09:46:19	test_spec_bank	SearchableRepository.search	PERFORMANCE	3
07-16-2014 09:35:34	test_spec_bank	TenancyService.getApplicableTenants	PERFORMANCE	72
07-16-2014 09:35:34	test_spec_bank	RolesAndPermissionsService.createUser	PERFORMANCE	172

To search for component metrics:

1. On the home screen (see Figure 2), click the View Metrics icon. Alternatively, select the View Metrics option from the menu. The ***Metric Search*** screen appears listing all the existing metrics for the deployed components.
2. Enter any search criteria you want to include using the available search filters. The different search filters are described in Table 4.
3. Click the [**Search**] button. The screen will display the search results table containing the metrics that match the search criteria.

Table 4: Metrics Search Screen Search Filters

Search Filter	Description
Start Date	Refers to the date when the metric was started. You can select the specific date from the calendar that is displayed when you place your cursor in the text box.
End Date	Refers to the date when the metric ended. You can select the specific date from the calendar that is displayed when you place your cursor in the text box.
Component	Refers to the component for which the metric was generated. You can select the component from the drop-down list that displays the names of all the components for which metrics have been generated.
Metric Type	Refers to the type of metrics that have been recorded for the component. You can select the required type from the drop-down list. The available options are: • Availability: Used to determine a component's availability. • Performance: Used to determine a component's performance and activities. • Throughput: Used to determine the database performance of a component. • Utilization: Used to determine a component's utilization of resources.
Name	Refers to the name of the metric. You can only search by the complete metric name.
Value	Refers to the metric value. For example, the value can indicate the time taken to perform an action. The value is metric- and component-specific and can refer to a unit of time, a unit of size, or a unit of objects.

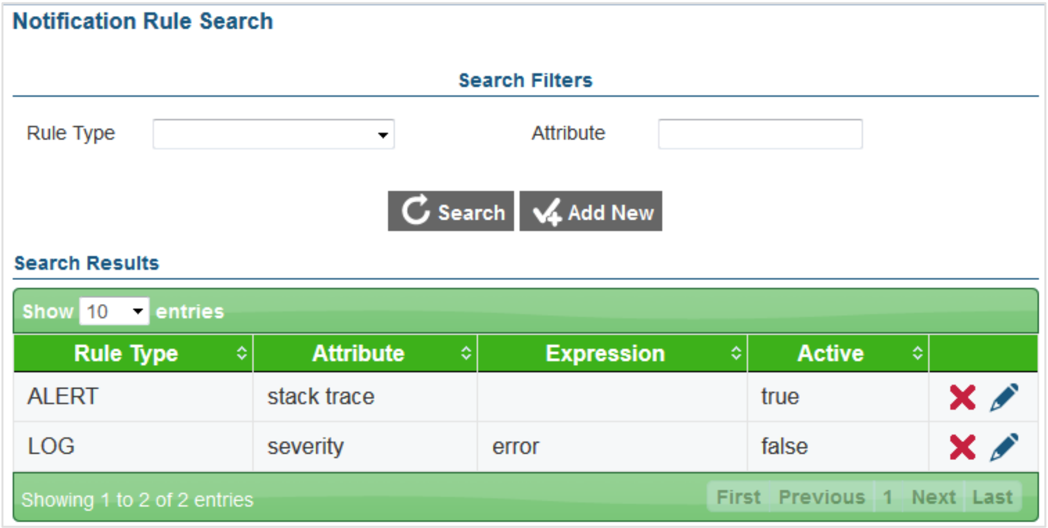
Managing Notification Groups

The Monitoring and Alerting System enables you to create groups of personnel to whom notification emails can be sent in case an alert or log generated for a component meets the user-specified notification criteria. From the ***Notification Group Search*** screen (see Figure 10), authorized users can search for, create, and manage notification groups.

To receive notifications, you must first set up notification rules that specify the alert or log criteria that must be met for emails to be sent. For information on setting up notification rules, refer to Managing Notification Rules

The Monitoring and Alerting System enables you to create rules for sending out notification emails. Notification emails are sent to specified groups only when these rules are met. You can set up rules for both logs and alerts. From the ***Notification Rule Search*** screen (see Figure 13), authorized users can search for, create, and manage notification rules.

Figure 13. Notification Rule Search Screen



Rule Type	Attribute	Expression	Active	
ALERT	stack trace		true	✗ ✎
LOG	severity	error	false	✗ ✎

Search for a Notification Rule

The ***Notification Rule Search*** screen lists all the existing notification rules.

To search for notification rules:

1. On the home screen (see Figure 2), click the Create/Modify Notification Rules icon. Alternatively, select the Create/Modify Notification Rules option from the menu. The ***Notification Rule Search*** screen appears listing all the existing rules.
1. On the ***Notification Group Search*** screen, enter any search criteria you want to include. The search criteria fields are described in Table 5.
2. Click the [**Search**] button. The screen will display the search results table containing the rules that match the search criteria.

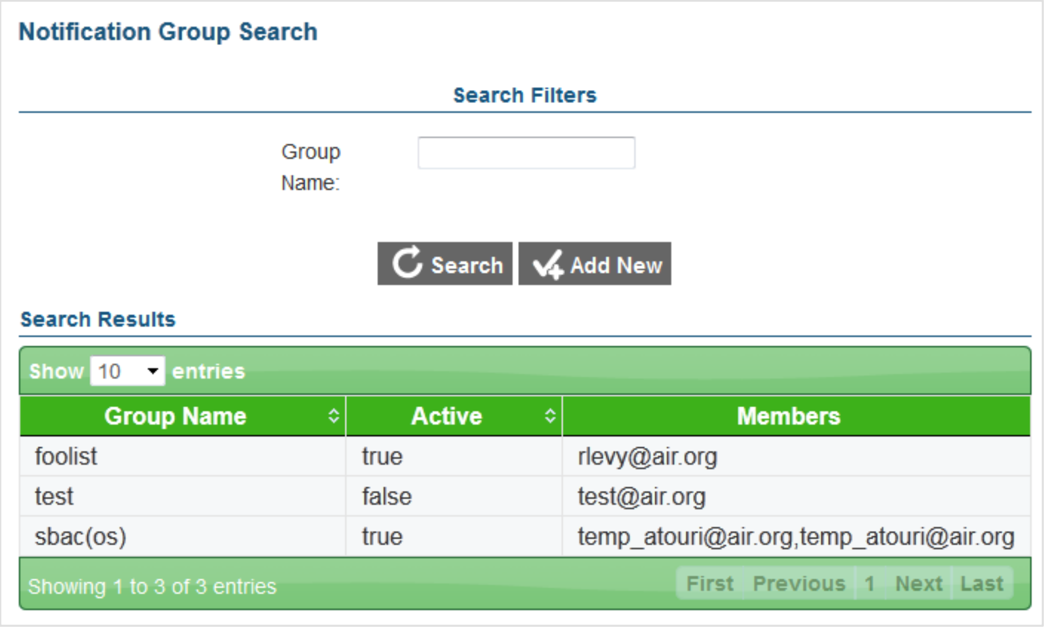
Add a Notification Rule

From the ***Notification Rule Search*** screen, you can add new notification rules or criteria based on which notification emails can be sent to specified groups.

Notification emails are only sent for rules that are marked as active and to groups that are marked as active. If a notification rule is inactive or if the group to whom the notification email should be sent is inactive, notification emails will not be sent.

Figure 14. Add Notification Rule Popup Window

Figure 10. Notification Group Search Screen



Group Name	Active	Members
foolist	true	rlevy@air.org
test	false	test@air.org
sbac(os)	true	temp_atouri@air.org,temp_atouri@air.org

Showing 1 to 3 of 3 entries

Search for a Notification Group

The ***Notification Group Search*** screen lists all the existing notification groups. You can search for a notification group or groups by the group name.

To search for notification groups:

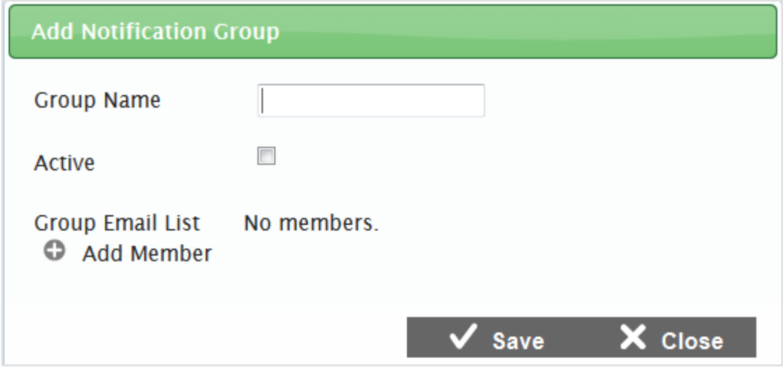
4. On the home screen (see Figure 2), click the Create/Modify Notification Groups icon. Alternatively, select the Create/Modify Notification Groups option from the menu. The ***Notification Group Search*** screen appears listing all the existing groups.
5. On the ***Notification Group Search*** screen, enter the group name. You can also enter partial names.
6. Click the [**Search**] button. The screen will display the search results table containing the groups that match the search criteria.

Add a Notification Group

From the ***Notification Group Search*** screen, you can add new notification groups to whom emails should be sent.

> ⚠ A notification group must consist of at least one member. Furthermore, notification emails are only sent to groups that are marked as active. If a group is inactive, notification emails will not be sent to the group even if the specified notification criteria are met.

Figure 11. Add Notification Group Popup Window



Add Notification Group

Group Name

Active □

Group Email List No members.

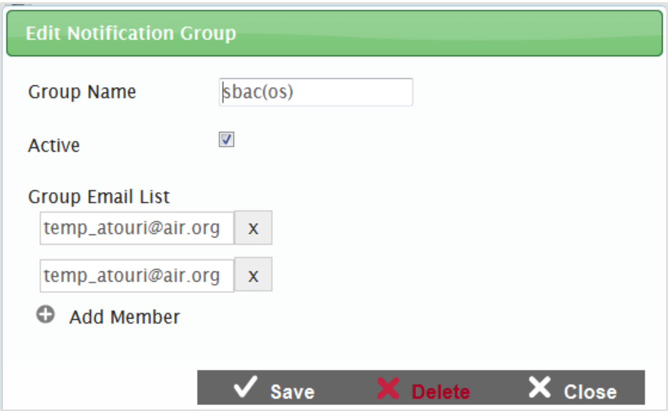
To add a notification group:

1. On the ***Notification Group Search*** screen (see Figure 10), click the [**Add New**] button. The Add Notification Group Popup Window appears.
2. In the *Group Name* field, enter the group's name.
3. To make the group active, check the checkbox in the *Active* field.
4. To add a member to the group, click the add [⊕] button. A row containing a text box will be displayed where you can add the group member's email address.
5. Enter the group member's email address.
6. Repeat the above two steps to add more members to the group. To remove a member from the group, click the delete [X] button next to the member's email.
7. To save the notification group, click the [**Save**] button. Verify that the new notification group is listed on the ***Notification Group Search*** screen.

Edit a Notification Group

You can edit a notification group if necessary. You can edit the name of the notification group, add or delete members, and modify the status of the group.

Figure 12. Edit Notification Group Popup Window


Edit Notification Group

Group Name: sbac(os)

Active ☑

Group Email List
temp_atouri@air.org x
temp_atouri@air.org x

To edit a notification group:

1. From the ***Notification Group Search*** screen (see Figure 10), search for the group you want to edit.
2. Double-click the selected row. The Edit Notification Group Popup Window appears.
3. Update the information as necessary. All fields are editable.
4. To save the update, click the [**Save**] button.

Delete a Notification Group

You can also delete a notification group if the group is no longer required.

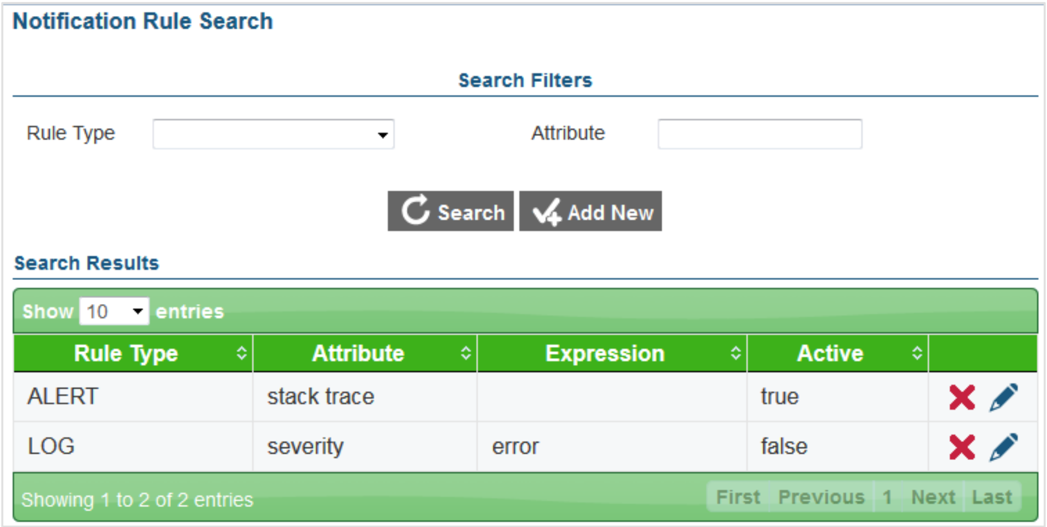
To delete a notification group:

1. From the ***Notification Group Search*** screen (see Figure 10), search for the group you want to delete.
2. Double-click the selected row. The Edit Notification Group Popup Window (see Figure 12) appears.
3. To delete the group, click the [**Delete**] button.

Managing Notification Rules

The Monitoring and Alerting System enables you to create rules for sending out notification emails. Notification emails are sent to specified groups only when these rules are met. You can set up rules for both logs and alerts. From the ***Notification Rule Search*** screen (see Figure 13), authorized users can search for, create, and manage notification rules.

Figure 13. Notification Rule Search Screen



Notification Rule Search

Search Filters

Rule Type

Attribute

Search Results

Show 10 entries

Rule Type	Attribute	Expression	Active	
ALERT	stack trace		true	✗ ✎
LOG	severity	error	false	✗ ✎

Showing 1 to 2 of 2 entries

Search for a Notification Rule

The ***Notification Rule Search*** screen lists all the existing notification rules.

To search for notification rules:

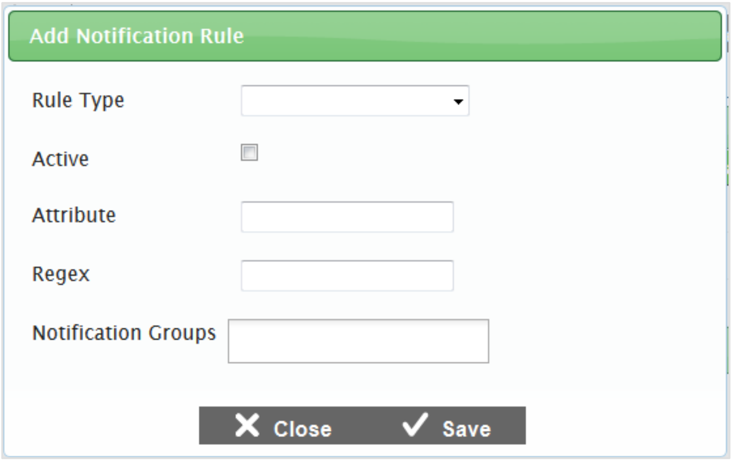
4. On the home screen (see Figure 2), click the Create/Modify Notification Rules icon. Alternatively, select the Create/Modify Notification Rules option from the menu. The ***Notification Rule Search*** screen appears listing all the existing rules.
5. On the ***Notification Group Search*** screen, enter any search criteria you want to include. The search criteria fields are described in Table 5.
6. Click the [**Search**] button. The screen will display the search results table containing the rules that match the search criteria.

Add a Notification Rule

From the ***Notification Rule Search*** screen, you can add new notification rules or criteria based on which notification emails can be sent to specified groups.

Notification emails are only sent for rules that are marked as active and to groups that are marked as active. If a notification rule is inactive or if the group to whom the notification email should be sent is inactive, notification emails will not be sent.

Figure 14. Add Notification Rule Popup Window


Add Notification Rule

Rule Type

Active □

Attribute

Regex

Notification Groups

To add a notification rule:

7. On the ***Notification Rule Search*** screen (see Figure 13), click the [**Add New**] button. The Add Notification Rule Popup Window appears.
8. Specify the notification rule details. The different fields are described in Table 5.
9. To save the notification rule, click the [**Save**] button. Verify that the new notification rule is listed on the ***Notification Rule Search*** screen.

Table 5: Notification Rule Detail Fields

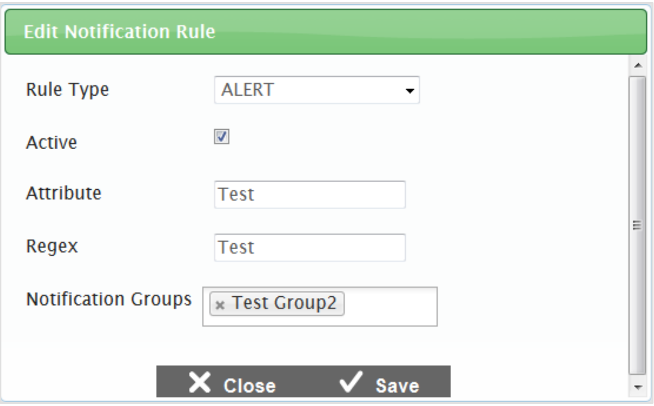
Field	Description
Rule Type	Refers to the entity with which the rule is associated. You can set up notification rules for component alerts as well as logs. You can select the required entity from the drop-down list that displays the two available options: • Alert • Log
Active	Indicates whether the rule is active. To activate the rule, check the checkbox.

Field	Description
Attribute	Refers to the log or alert field on which the notification rule should be performed. You can enter the required attribute in the text box provided. The attributes are dependent on the selected rule type. The available attributes are: • Alert: ○ severity ○ message ○ alertType • Log: ○ severity ○ message ○ stackTrace ○ referenceNumber
Regex	Regex or Regular Expression refers to a specialized syntax for matching patterns in strings. You can enter the required regular expression, which is matched against the value of the attribute specified for the rule. If the attribute value matches the regular expression, notification emails can be sent. For more information on regular expression, refer to http://docs.oracle.com/javase/7/docs/api/java/util/regex/Pattern.html.
Notification Groups	Refers to the groups to which notification emails should be sent in case the rule criteria are met. You can select the required notification group from the drop-down list. The list is only displayed after you start typing. For example, if you enter “c,” a list of all notification groups whose name contains the letter “c” appears. You can also remove a notification group from the list by clicking the delete [x] button next to the group.

Edit a Notification Rule

You can edit a notification rule if necessary. For example, if you want to receive notification alerts for a particular rule on specific days only, you can activate the rule on the required day and keep it deactivated at other times. You can edit all the details, such as the entity with which the rule is associated and the status of the rule. You can also add or delete the groups to whom notification emails should be sent.

Figure 15. Edit Notification Group Popup Window



Edit Notification Rule

Rule Type: ALERT

Active: ☑

Attribute: Test

Regex: Test

Notification Groups: × Test Group2

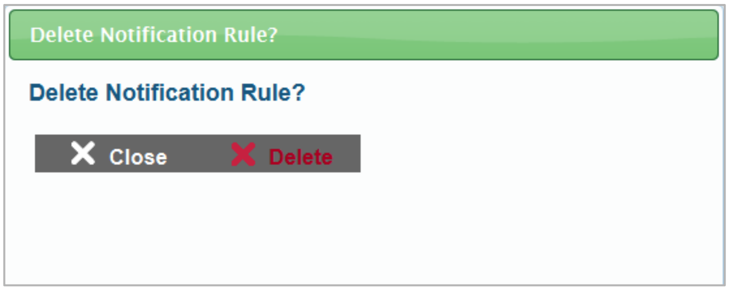
To edit a notification rule:

10. From the ***Notification Rule Search*** screen (see Figure 13), search for the rule you want to edit.
11. Click the [✎] button. The Edit Notification Rule Popup Window appears.
12. Update the information as necessary. All fields are editable.
13. To save the update, click the [**Save**] button.

Delete a Notification Rule

You can also delete a notification rule if the rule is no longer required.

Figure 16. Delete Notification Rule Popup Window



Delete Notification Rule?

Delete Notification Rule?

To delete a notification rule:

14. From the ***Notification Rule Search*** screen (see Figure 13), search for the rule you want to delete.
15. Click the [✕] button. The Delete Notification Rule Popup Window (see Figure 16) appears.
16. To delete the rule, click the [**Delete**] button.