

HCL Detect v12.1.8 Admin Guide



Contents

- Chapter 1. Introduction..... 3
- Chapter 2. User & Role Management..... 4
- Chapter 3. System Health..... 15
- Chapter 4. Applications, Aggregates & Enrichments..... 17
- Chapter 5. Subscriber Segments.....24

Chapter 1. Introduction

This guide helps administrators to configure user roles and permissions, monitor feed applications and system health, and manage subscriber segments. The administrator can access the Administration menu in the Header to navigate to User roles and management, System health and Settings option to manage the application.

Chapter 2. User & Role Management

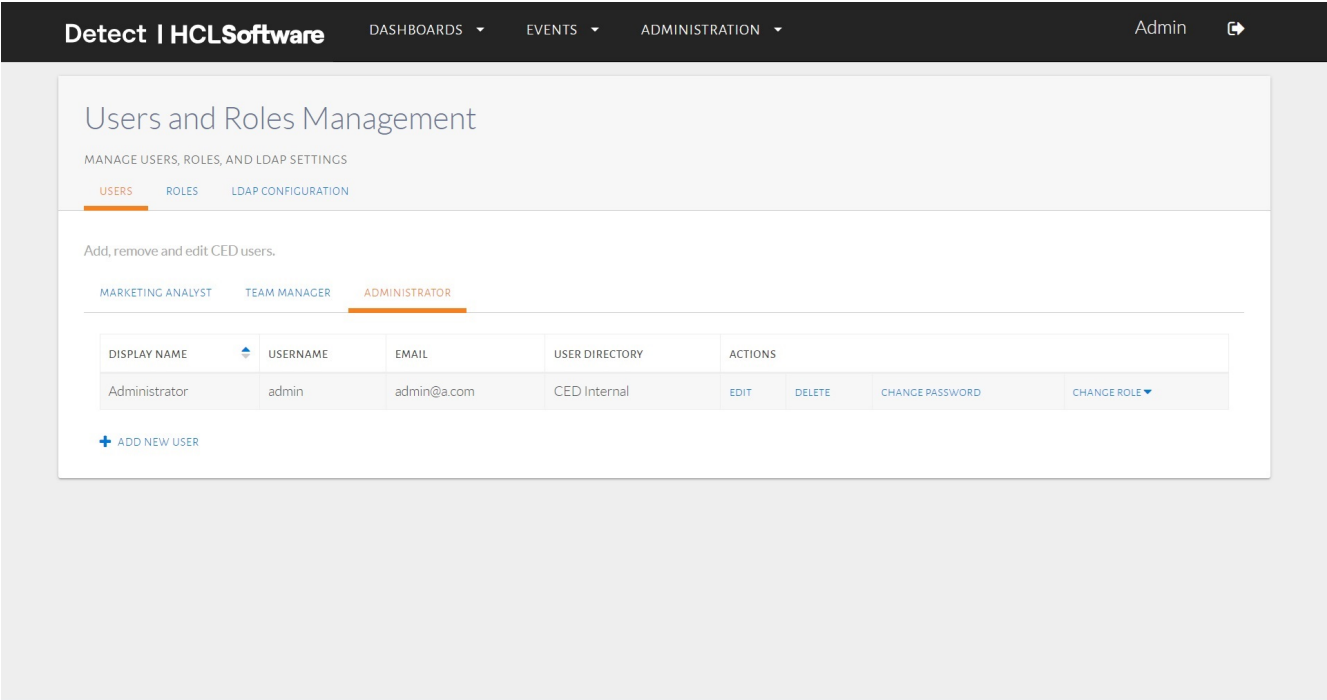
The only user that comes pre-configured with HCL Detect is the `admin` user.

The `admin` user can add additional users, including other administrators, as well as perform other user management tasks by accessing the

User And Role Management

link located under the `Administration` category in the top navigation bar.

The user management screen is shown below:



The `UserAndRoleManagement` page.

In the `Users` tab, the various roles that are configured in the system and the users that exist for each such role are depicted.

To add a new user, the administrator must first decide the role for such a user, for example, the `MarketingAnalyst` role can be selected by picking the corresponding tab in the `User Management` page and by clicking on the `Add New User` link:

The screenshot displays the 'Detect | HCLSoftware' user management interface. The top navigation bar includes 'DASHBOARDS', 'EVENTS', and 'ADMINISTRATION' menus, with the 'Admin' user profile on the right. The main section is titled 'MANAGE USERS, ROLES, AND LDAP SETTINGS' and contains tabs for 'USERS', 'ROLES', and 'LDAP CONFIGURATION'. Below this, a sub-header reads 'Add, remove and edit CED users.' and features role selection tabs: 'MARKETING ANALYST', 'TEAM MANAGER', and 'ADMINISTRATOR'. The 'ADD NEW USER' form is visible, with fields for USERNAME, EMAIL, FIRST NAME, LAST NAME, DISPLAY NAME, and PASSWORD. The USERNAME field is highlighted with a red border and a red error message: 'A valid username is required (alphanumeric, no spaces).'. A note below the USERNAME field states: 'The user's sign in username. This field is not editable.' The PASSWORD field has a 'SHOW' toggle and a note: 'The user password must be at least 6 characters in length, must contain at least one number, must contain at least one upper case letter.' At the bottom of the form are 'SAVE' and 'CANCEL' buttons.

Detect | HCLSoftware DASHBOARDS ▾ EVENTS ▾ ADMINISTRATION ▾ Admin ↗

MANAGE USERS, ROLES, AND LDAP SETTINGS

USERS ROLES LDAP CONFIGURATION

Add, remove and edit CED users.

MARKETING ANALYST TEAM MANAGER ADMINISTRATOR

ADD NEW USER

USERNAME A valid username is required (alphanumeric, no spaces).
The user's sign in username. This field is not editable.

EMAIL

FIRST NAME

LAST NAME

DISPLAY NAME
This is the name displayed to other users system wide.

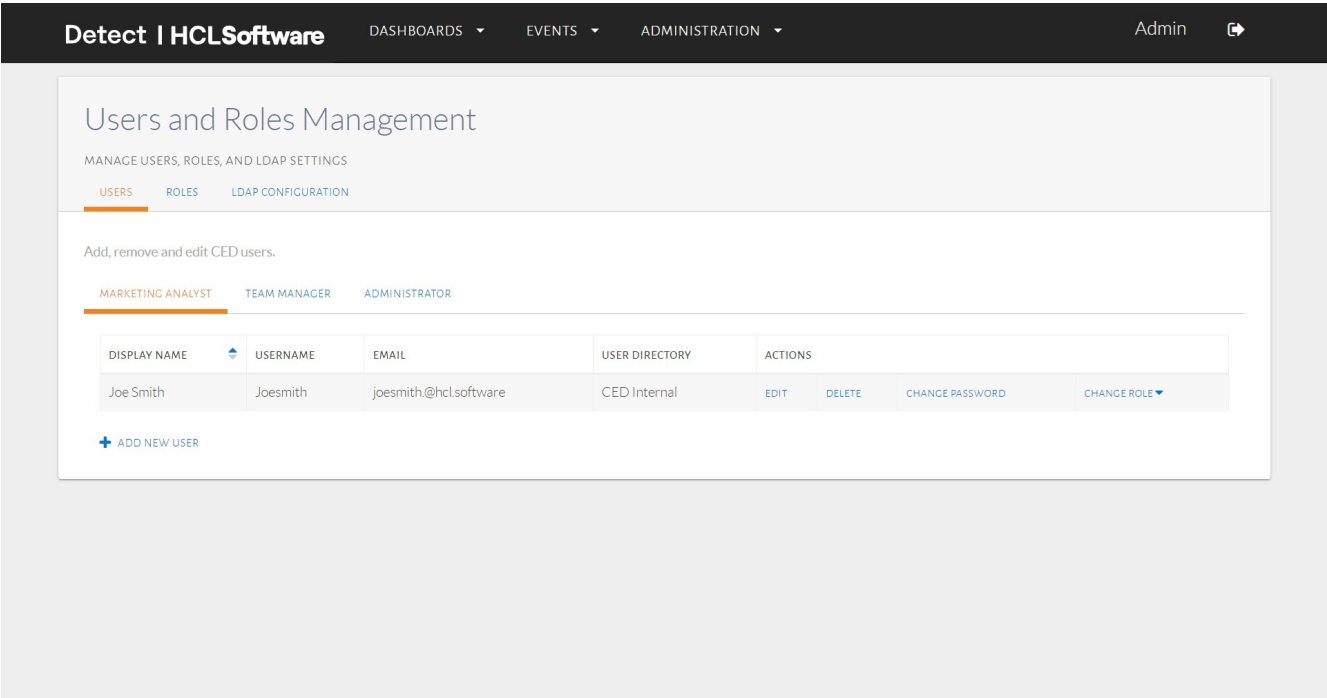
PASSWORD **SHOW**
The user password must be at least 6 characters in length, must contain at least one number, must contain at least one upper case letter.

SAVE **CANCEL**

Adding a new user.

Subsequently, the Username, Email, First Name, Last name, Display name and Password attributes should be filled out. Finally, the Save button can be pressed to store this data.

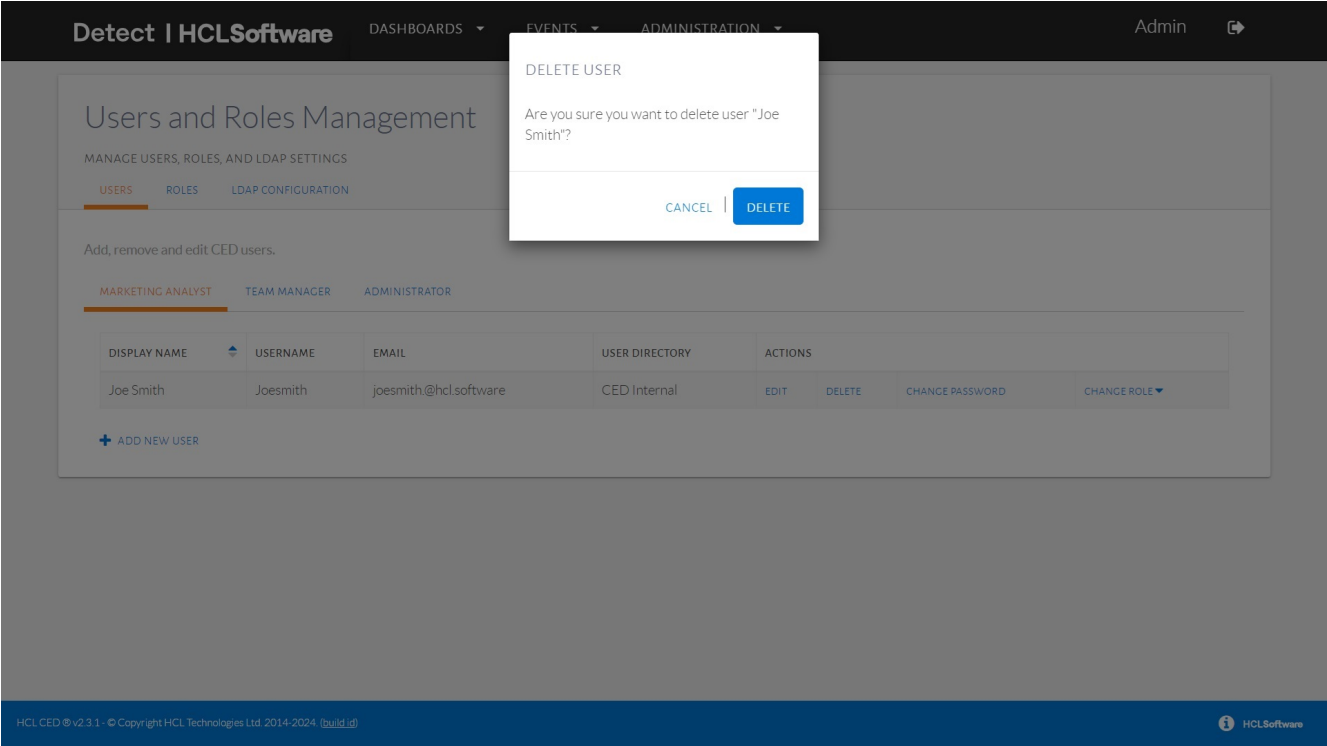
Once completed, the newly added user should be visible in the user interface:



A newly added user.

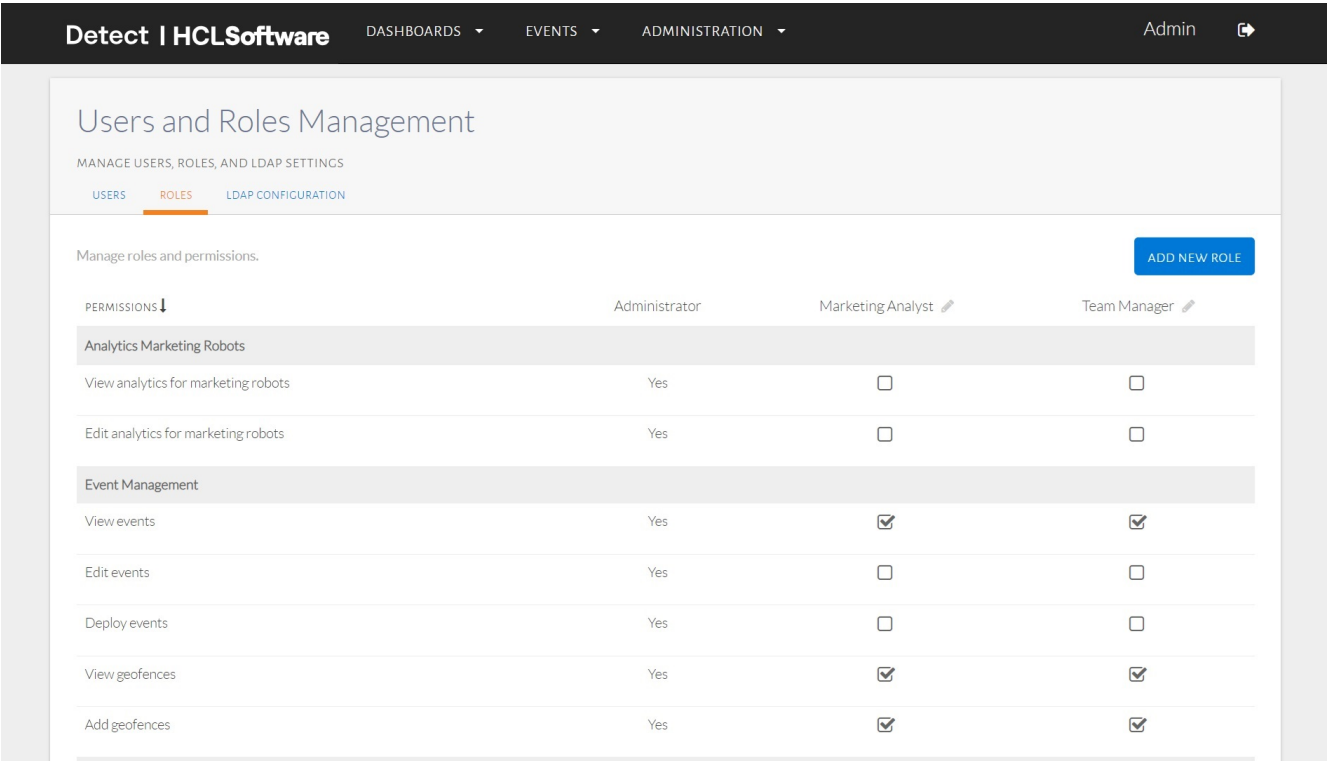
The data for an existing user can be modified and the user itself can be removed by another user with user management entitlement.

The deletion and editing are performed using `delete` and `Edit` button under `Actions` head of the table:



Removing or updating a user's data.

The Roles page can be accessed by accessing the Roles tab in the navigation bar:



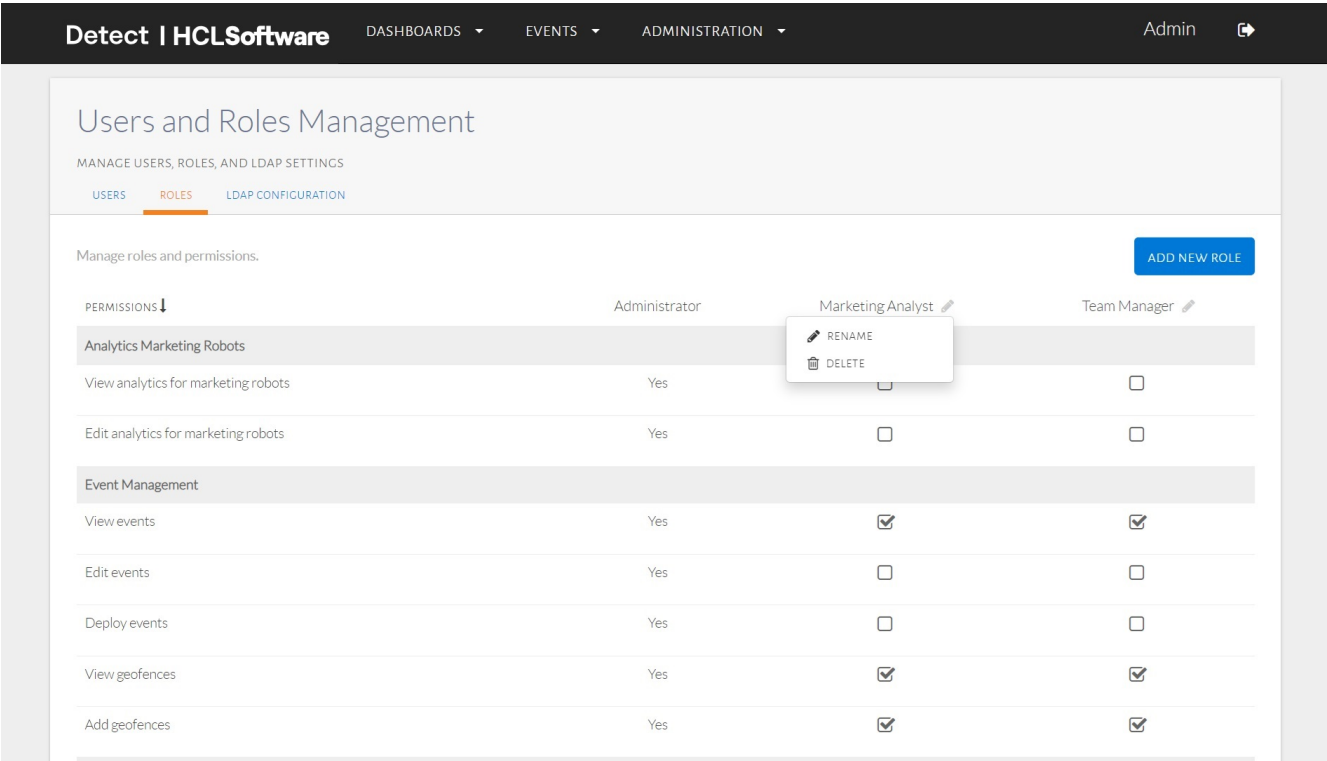
The `Roles` tab.

The HCL Detect, by default, comes with three default roles: the `Administrator`, the `Team Manager` and the `Marketing Analyst`:

- The `Administrator` has unrestricted permissions in HCL Detect.
- The `TeamManager` does not have the permissions associated with user and role management, but has all the other permissions.
- The `MarketingAnalyst` has permissions that are a notch below a `Team Manager`, excluding, for instance, the ability to edit the feeds.

Roles can be renamed and removed.

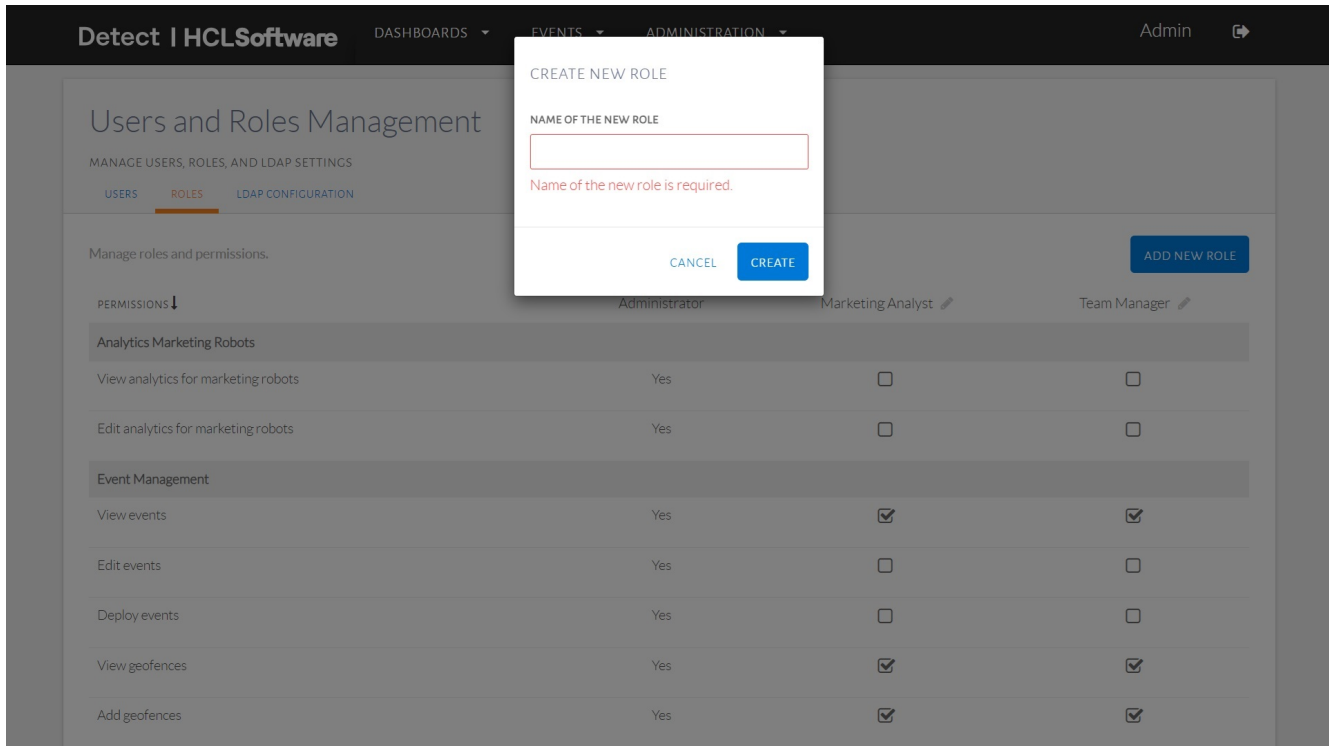
The removal of a role can only be accomplished if no user(s) with that role exists. The user interface shows an appropriate error when an attempt is made to delete a role that has user(s) assigned to it:



Renaming and deletion options for a role.

A new role can be created by clicking on the `AddNewRole` button located at the top-right corner.

The resulting pop-up asks the user to enter the name of the new role and, upon clicking on the `create` button, the corresponding new role is created.



Adding a new role.

A new role is created without any permissions. Permissions can then be added to the newly created role by clicking on the corresponding check-boxes:

Detect | HCLSoftware

DASHBOARDS ▾EVENTS ▾ADMINISTRATION ▾

Admin

Users and Roles Management

MANAGE USERS, ROLES, AND LDAP SETTINGS

USERSROLESLDAP CONFIGURATION

Manage roles and permissions.

ADD NEW ROLE

EDITING IN PROGRESS

SAVE

DISCARD CHANGES

PERMISSIONS ▾	Administrator	Event Manager	Marketing Analyst	Team Manager
Analytics Marketing Robots				
View analytics for marketing robots	Yes	☐	☐	☐
Edit analytics for marketing robots	Yes	☐	☐	☐
Event Management				
View events	Yes	☒	☒	☒
Edit events	Yes	☐	☐	☐
Deploy events	Yes	☐	☐	☐
View geofences	Yes	☐	☒	☒

A newly created role (Event Manager) with View events permissions only.

HCL Detect can be optionally configured to do LDAP based authentication. The LDAPConfiguration page can be used to configure the LDAP Configuration tab in the navigation bar:

Detect | HCLSoftware

DASHBOARDS ▾EVENTS ▾ADMINISTRATION ▾

Admin

Users and Roles Management

MANAGE USERS, ROLES, AND LDAP SETTINGS

USERSROLESLDAP CONFIGURATION

Manage LDAP integration.

LDAP integration has not been set up yet.

CONFIGURE AND ENABLE LDAP

The `LDAPConfiguration` tab.

To enable LDAP based authentication, we need to click on `ConfigureAndEnableLDAP` button:

Configuring the `LDAPConfiguration` tab.

Subsequently, the `ServerType`, `Hostname`, `Port`, `Base DN`, `User DN`, `Group DN`, `Search User Name` and `Search User Password` attributes should be filled out. Current two type are servers are supported, i.e., `Free IPA` and `Active Directory`. Finally, the `Test And Save` button can be pressed to test the server setting:

Detect | HCLSoftware

DASHBOARDS ▾EVENTS ▾ADMINISTRATION ▾

Admin ↗

✓ SERVER SETTINGS

✓ USER SCHEMA SETTINGS

SERVER TYPE

ActiveDirectory ▾

HOSTNAME

ipa.demo.hcl.com

Hostname for the ActiveDirectory LDAP server (e.g. ipa.demo.hcl.com).

PORT

389

The port on which the LDAP server is listening (e.g. 636).

Use SSL

Verify SSL Certificate

This will encrypt the connection between CED and your LDAP server.

This will ensure that a valid SSL certificate is used for your connection.

BASE DN

dc=unicindia,dc=com

Root node in LDAP from which to search users (e.g. dc=demo,dc=hcl,dc=com).

USER DN

cn=Users

This is prepended to your Base DN to limit the scope when searching for users (e.g. cn=users,cn=accounts).

GROUP DN

This is prepended to your Base DN to limit the scope when searching for users (e.g. cn=groups,cn=accounts).

SEARCH USER NAME

unicindia\administrator

This is the user name that will be used for authentication of the user search (e.g. uid=test,cn=users,cn=accounts,dc=demo,dc=hcl,dc=com).

SEARCH USER PASSWORD

This is the password that will be used for authentication of the user search.

SHOW ADVANCED SETTINGS

DISCARD CHANGES

TEST AND SAVE

No changes to save

TEST CURRENT SETTINGS

NEXT

Testing the `ServerSettings`.

Press `Next` Button to start configuring the `User Schema Settings` tab. Now `user Object Class`, `User Object Filter`, `Username Attribute`, `User Name RDN Attribute`, `User First Name Attribute`, `User Lastname Attribute`, `User Display Name Attribute`, `User Email Attribute` and `User Distinguished Name Attribute` attribute needs to be filled based on your organization's LDAP configurations:

Detect | HCLSoftware DASHBOARDS ▾ EVENTS ▾ ADMINISTRATION ▾ Admin ↗

✓ SERVER SETTINGS ✓ **USER SCHEMA SETTINGS**

USER OBJECT CLASS
The LDAP user object class type to use when loading users (e.g., inetorgperson).

USER OBJECT FILTER
The filter to use when searching for user objects (e.g., (objectClass=inetorgperson)).

USERNAME ATTRIBUTE
The object attribute to use when loading the user's sign in username (e.g., uid).

USER NAME RDN ATTRIBUTE
The RDN to use when loading the username (e.g., uid).

USER FIRST NAME ATTRIBUTE
The object attribute to use when loading the user's first name (e.g., givenName).

USER LAST NAME ATTRIBUTE
The object attribute to use when loading the user's last name (e.g., sn).

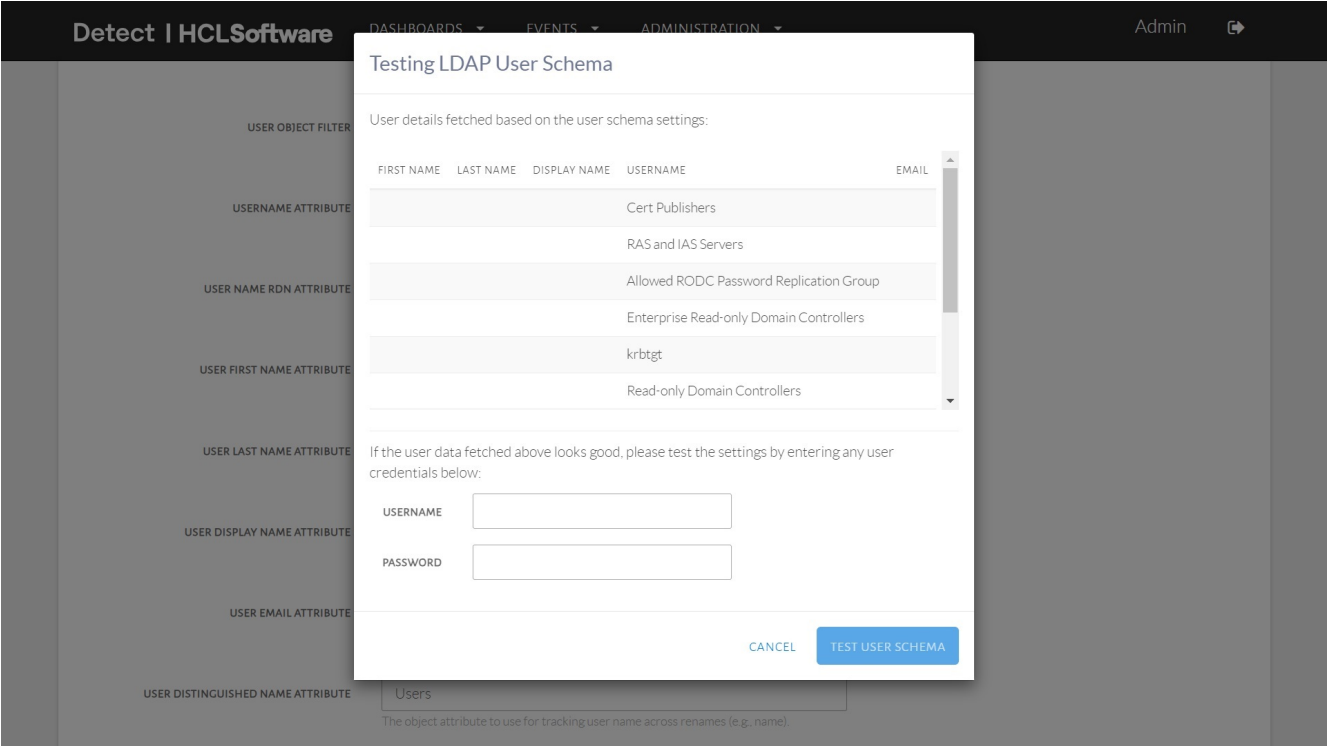
USER DISPLAY NAME ATTRIBUTE
The object attribute to use when loading the user's display name (e.g., displayName).

USER EMAIL ATTRIBUTE
The object attribute to use when loading the user's email (e.g., mail).

USER DISTINGUISHED NAME ATTRIBUTE
The object attribute to use for tracking user name across renames (e.g., name).

Configuring the `UserSchemaSettings`.

Now Click on `TestAndSave` button to test the configuration. Test it by filling `Username` and `Password` for any existing LDAP user and clicking `Test And Save` on the pop-up display.



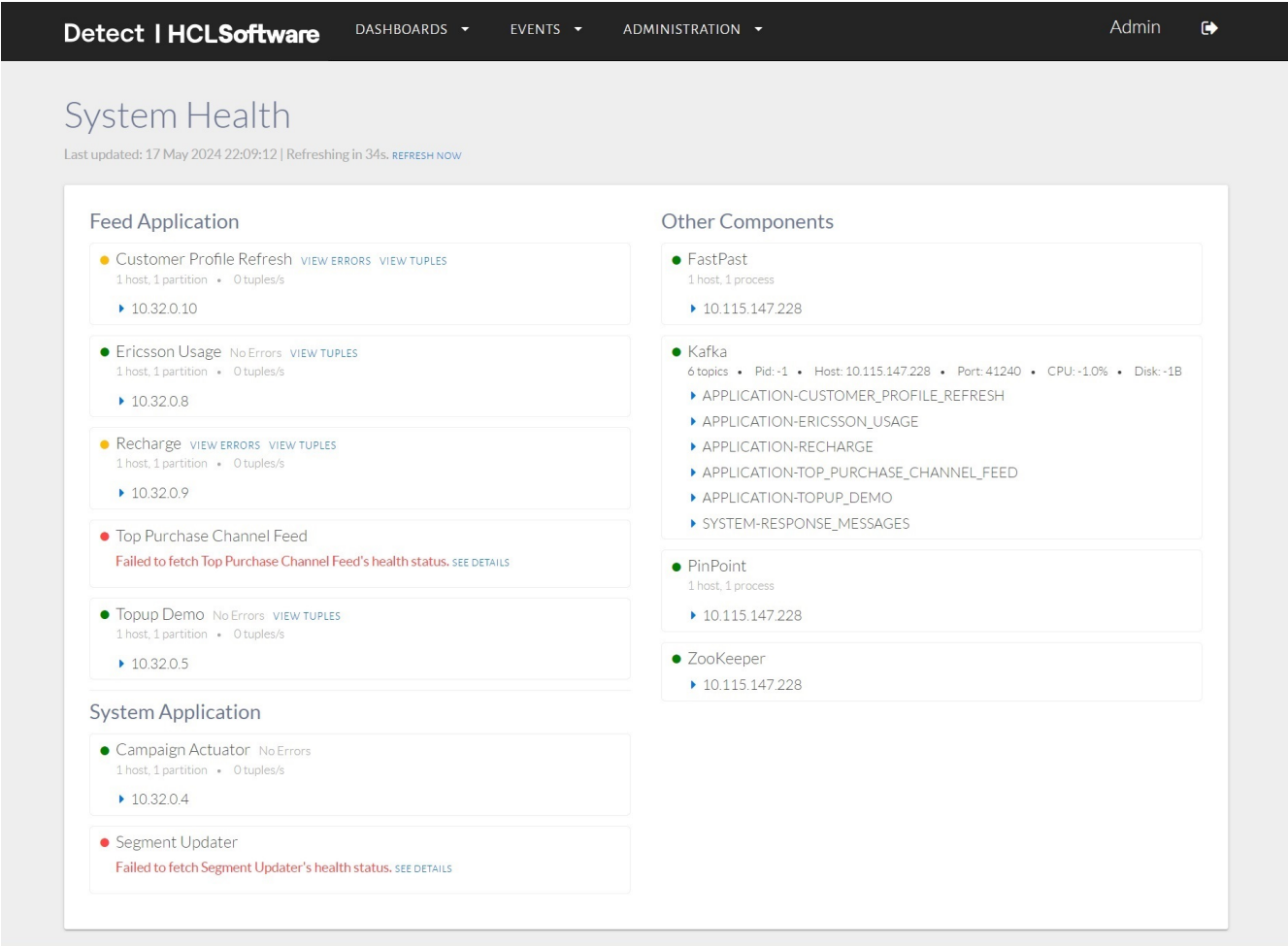
Testing the UserSchemaSettings.

Chapter 3. System Health

The `systemHealth` dashboard can be accessed by clicking on the `System Health` link in the top navigation bar.

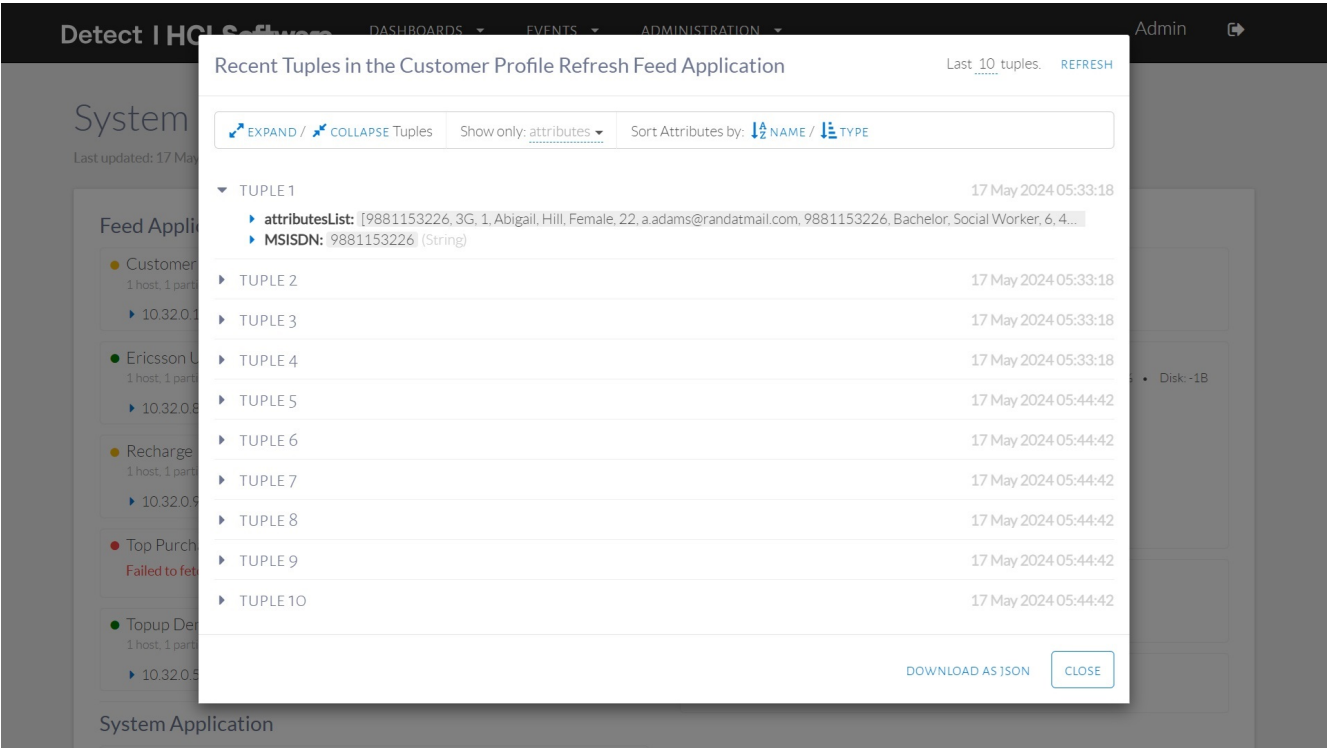
The dashboard shows the status of the `AnalyticsApplications`, `Feed Applications`, `System Applications` and `Other Components`.

`FeedApplications` are used for ingesting the incoming streaming data, `Analytics Applications` are used for stream or Batch based analytics jobs, `System Applications` are built-in applications used for different important functions of application like detecting events or managing batch segment updates. `Other Components` are the HCL Detect supporting components, including the `FastPast`, the `PinPoint`, the `Kafka` and the `Zookeeper`:



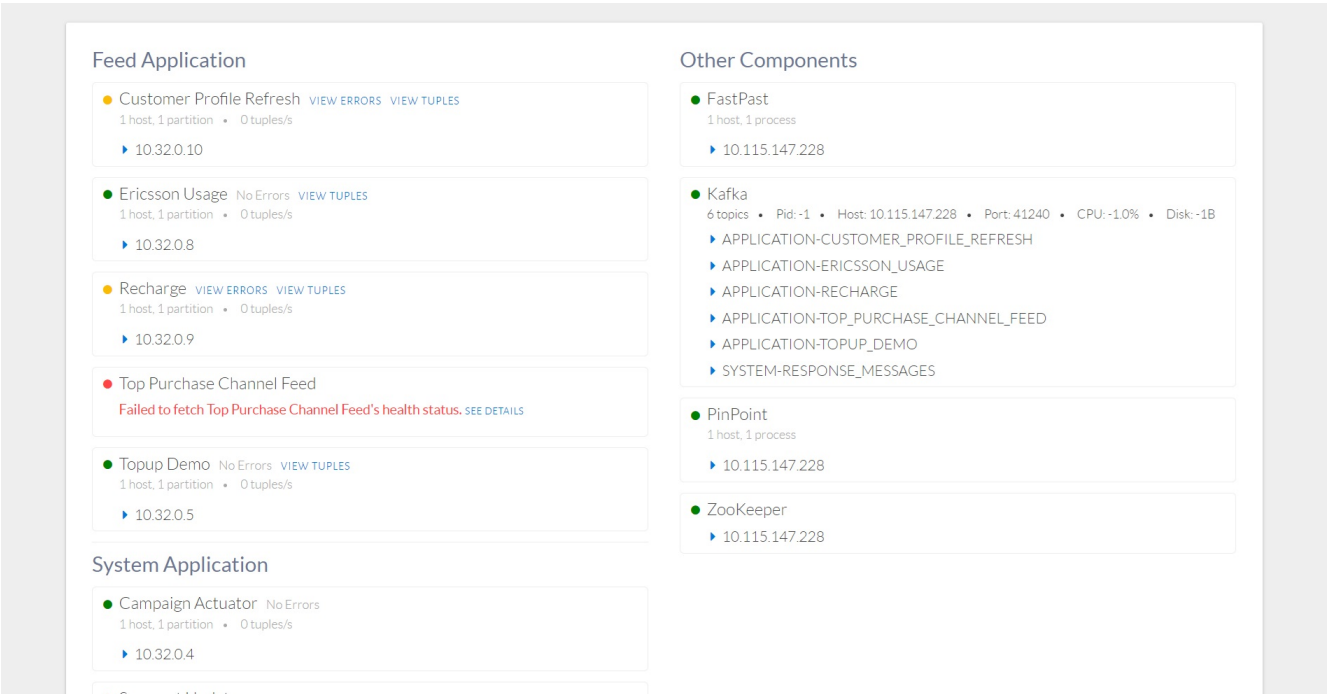
The `systemHealth` dashboard.

`FeedApplications` can also be used to see the last few data rows/tuples begin processed by clicking `View Tuples` button:



viewtuples from feed applications.

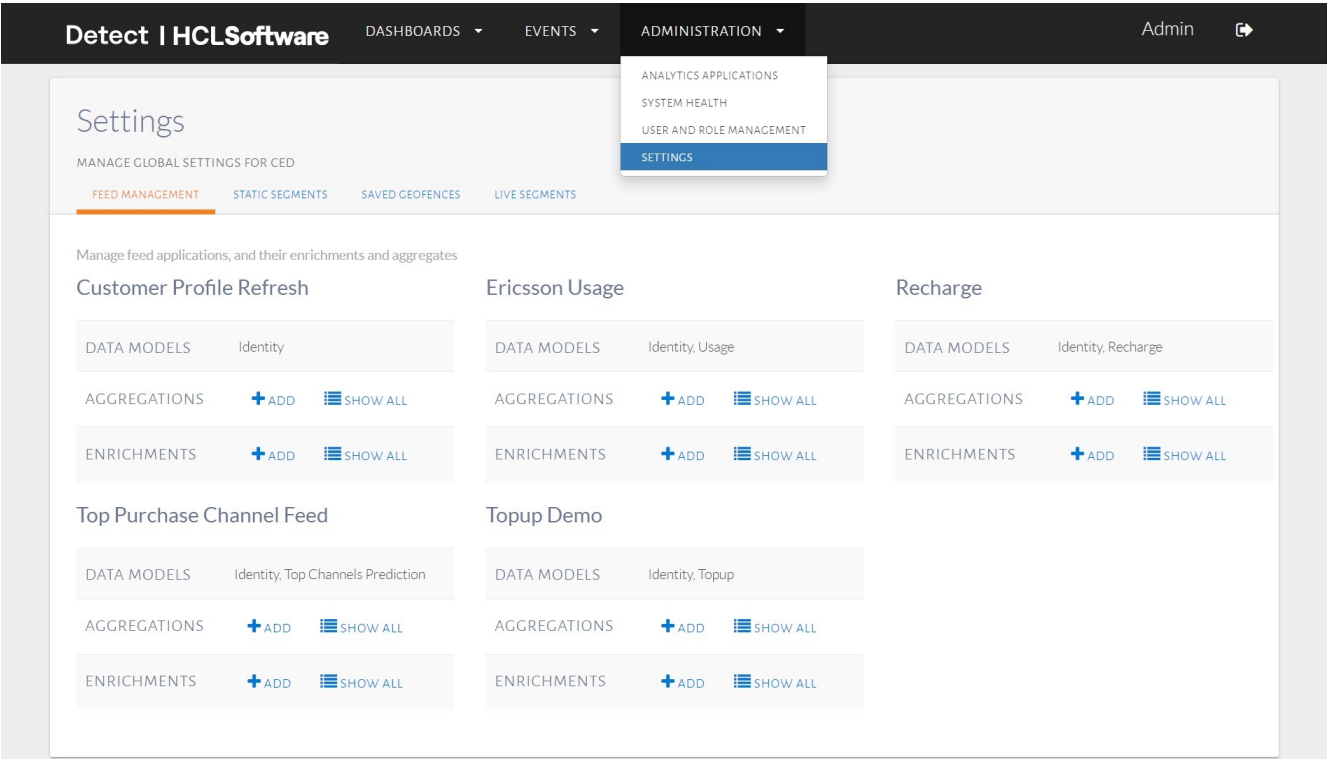
FeedApplications also shows the resource utilization of a feeds and parallel processing flow of each feeds.



partitions and statistics of a feed application.

Chapter 4. Applications, Aggregates & Enrichments

All of the feed applications configured in HCL Detect can be seen by clicking on the `Administration` link in the top navigation bar and then by clicking the `Settings` menu item. We have to use `Feed Management` tab to see feed applications.



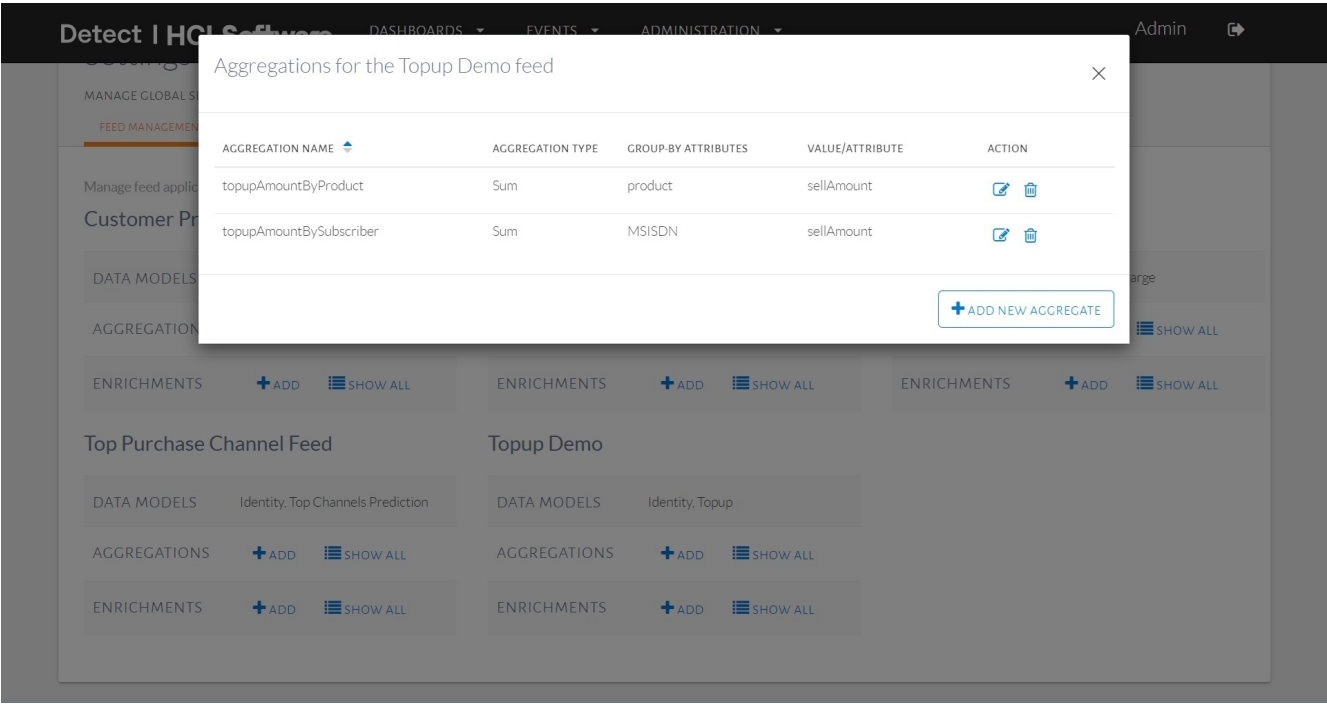
The applications configured in HCL Detect.

This dashboard shows the applications and their associated data model, e.g., 'Topup', 'Usage', etc.

Users with the appropriate permissions can use this page to view, edit, add and/or delete the aggregates and enrichments associated with a given feed application.

The existing aggregates configured for a feed application can be seen by clicking on the `ShowAll` button in the `Aggregations` row for that application.

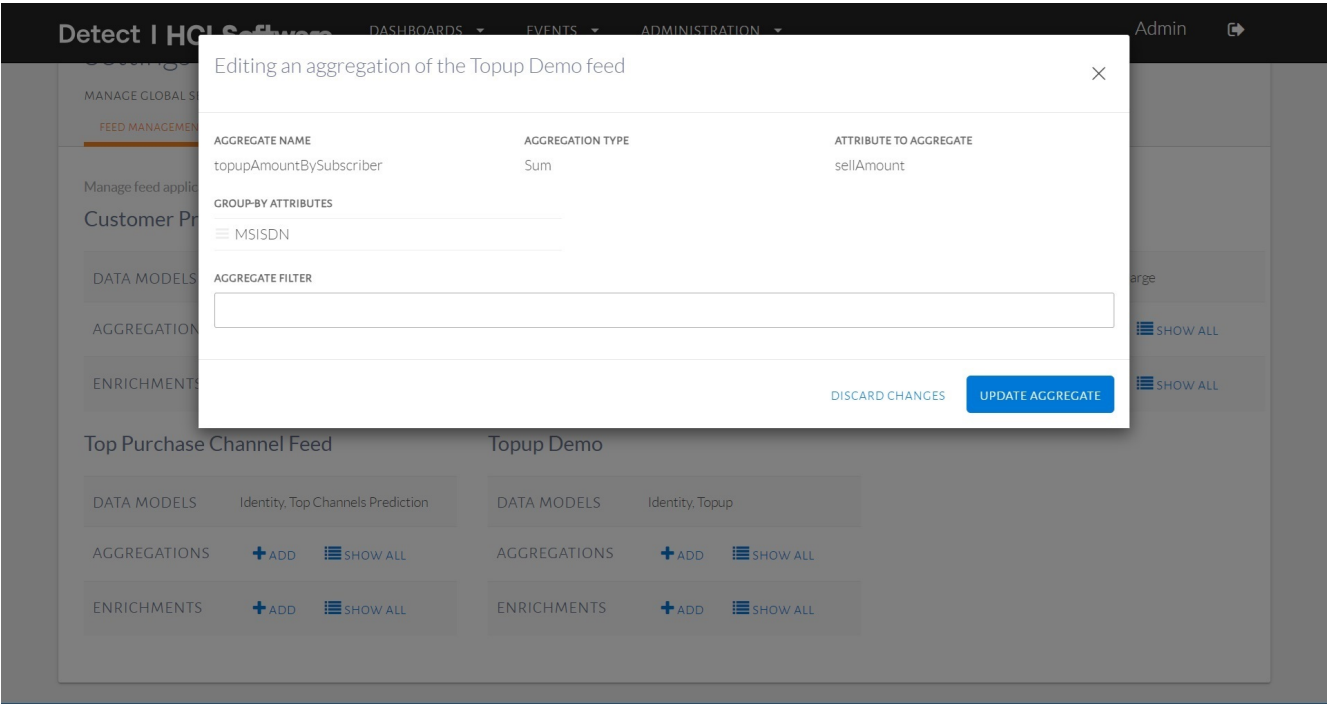
The dialog showing the aggregates associated with the `TopupDemo` application is below:



The aggregates associated with the TopupDemo feed.

The aggregates associated with a feed can be edited and removed.

To explain the aggregates a bit further, let us consider the aggregate called `topupAmountBySubscriber`. The dialog that opens up upon clicking on the edit button is shown below:



Editing an aggregate.

This aggregate is designed to count the number of calls by subscriber over various time windows (e.g., `currentDay`, `lastDay`, etc.).

`topupAmountBySubscriber`, i.e. the aggregate `Name`, is the name that is used to refer to the aggregate when using it in a trigger.

The `AggregationType`, in this case `Sum`, is used to accumulate the topup amounts, and the group-by attribute, in this case, `MSISDN`, is used to produce per-user tallies, since it identifies individual subscribers.

Additional group-by attributes can be added in a manner similar to the *group-by* clause used in traditional relational database management system (RDBMS) query languages.

A filter condition can also be used when only a subset of tuples is to be considered for an aggregation.

For instance, if the incoming tuples in the feed contain a Boolean `isDroppedCall`, indicating a dropped call, then one can calculate `droppedCallsBySubscriber` by using `isDroppedCall` equals to `True` as a filter condition with the `MSISDN` as the group-by attribute and `count` as the aggregation type.

To add a new aggregate, we need to click on `Add` button for that feed application. A dialog with form needs to be filled by filling `Aggregate Name`, `Aggregation Type`, `Attribute to Aggregate`, `Group by Attribute` and `Aggregation Filter`:

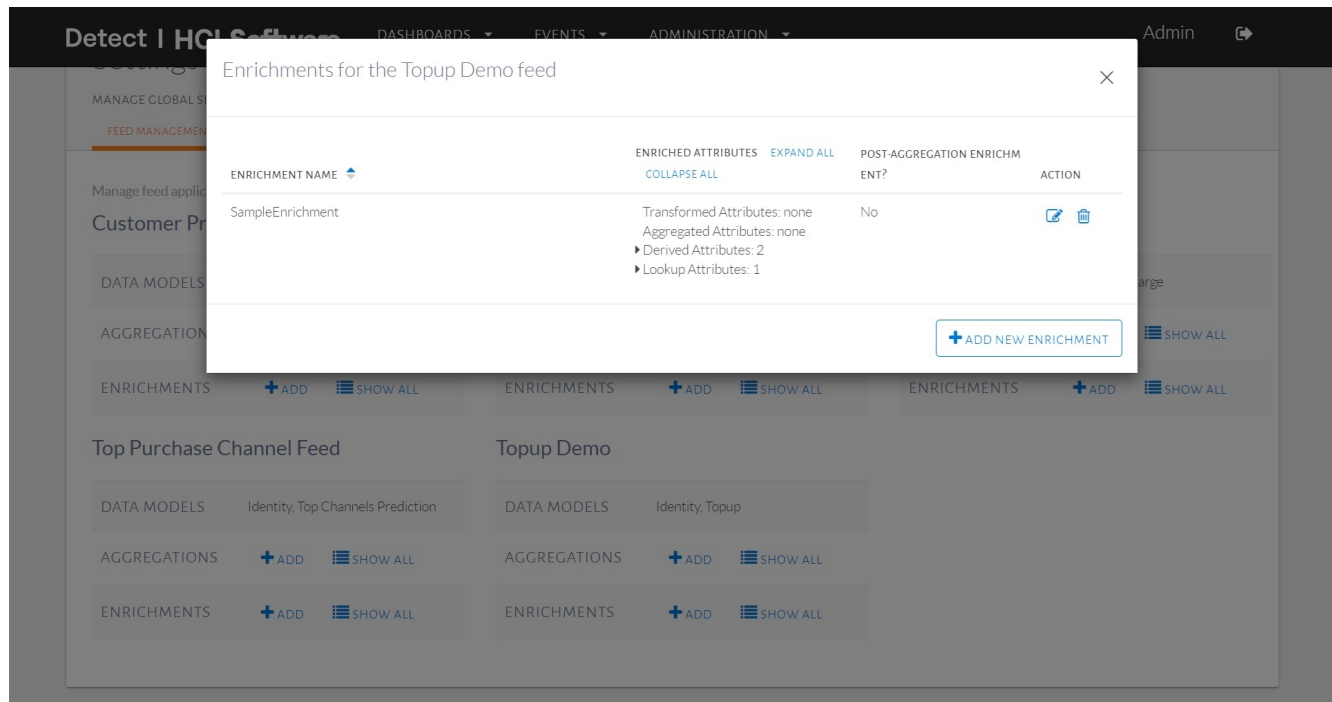
The screenshot shows a web application interface for 'Detect | HCL Software'. A modal dialog titled 'Adding an aggregation to the Topup Demo feed' is open. The dialog has the following fields and options:

- AGGREGATE NAME:** A text input field containing 'nameofAggregate'.
- AGGREGATION TYPE:** A dropdown menu currently showing 'filter items'. A list of options is visible: Count, Sum, Minimum, Maximum, Average, and Variance.
- ATTRIBUTE TO AGGREGATE:** A dropdown menu showing 'sellAmount'.
- GROUP-BY ATTRIBUTES:** A section containing a text input field with 'MSISDN' and a dropdown menu with 'product'. An 'ADD' button is next to the dropdown.
- AGGREGATION FILTER:** An empty text input field.
- Buttons:** 'DISCARD CHANGES' and 'CREATE AGGREGATE' at the bottom right.

The background interface shows a sidebar with 'FEED MANAGEMENT' selected, and a table of feeds with columns for 'DATA MODELS', 'AGGREGATIONS', and 'ENRICHMENTS'. The 'Top Purchase' feed is highlighted.

Adding new aggregate to a feed.

The list of enrichments associated with a feed can be seen by clicking on the `Show` button in the `Enrichments` row. The enrichments associated with the `Topup Demo` feed can be seen below:



The enrichments associated with the `TopupDemo` feed.

HCL Detect supports 4 kinds of enrichments:

- The *transformed attributes* enrichment enables one to add attributes to the tuple that have either a constant value or a value that can easily be derived from an UEL expression. Such transformed attribute may be needed by other enrichments or retained as an attribute in the enriched tuple. Note that retaining and forwarding the constant attributes as part of the output tuple from the enrichment step is optional.
- The *lookup-based* enrichment, which retrieves attributes from the profile store and possibly add them to the outgoing tuple. Note that retaining and forwarding the looked up attributes as part of the output tuple from the enrichment step is optional. We have to first select a key attribute present in the tuple, the associate `Pinpoint` table will be listed in `Lookup Table` drop-down, finally we have to select the attribute from the lookup table to be looked up.
- The *aggregate-based* enrichment, which fetches data from `FastPast` and possibly adds such attributes to the outgoing tuple. As part of configuring an aggregated attribute, it is necessary to (1) select an aggregate from the list of available aggregates for the feed, (2) select the window length unit, which can be `Minute`, `Hour`, `Day`, `Month` or `Year`, (3) select the period which can be one of `Current` or `Last` and (4) optionally select `Window length`, which can be used to indicate that only a subset of an aggregate is to be used. For instance, when the `Day` window length unit and the `Last` period with `Window Length` set to 7 is chosen, the aggregated value for the last 7 days can be computed. Note that when using the `Minute` window length unit, `Window Length` needs to be multiple of 10-minute i.e., backend configured sub-hour buckets length. Similarly to lookup-based enrichment, aggregate-based enrichment attributes may or may not be retained and forwarded as part of the output tuple.
- The *derived attributes* enrichment, which enables the execution of an external Python function. One such a function takes in a tuple (as well as any other required additional parameters, if any), performs a user-defined computation, and produces a result. This function invocation's return value can then be retained and forwarded as part of an

outgoing tuple. This capability can be used, for instance, to invoke a scoring function on an incoming tuple, which computes a score (e.g., based on previously mined data) that can then be added as an attribute to the corresponding outgoing tuple. The *derived attributes* enrichment are basically of three types, i.e., *enrichment function based*, *expression based* and *scorer function based*. *expression based* takes an UEL expression explained in Miscellaneous » UEL section.

The interface for editing enrichments is shown below:

Editing an enrichment of the Topup Demo feed

ENRICHMENT NAME: SampleEnrichment POST-AGGREGATION ENRICHMENT: No

TRANSFORMED ATTRIBUTES (0) LOOKUP ATTRIBUTES (1) AGGREGATED ATTRIBUTES (0) DERIVED ATTRIBUTES (2)

ATTRIBUTE NAME	LOOKUP TABLE	KEY ATTRIBUTE	LOOKED UP ATTRIBUTE	TYPE	RETAINED?
lastMSISDN	CUSTOMER_PROFILE	MSISDN	lastMSISDN	String	☐

ADD LOOKUP ATTRIBUTE

KEY ATTRIBUTE: No items selected ▼

LOOKUP TABLE: Please select a key attribute first

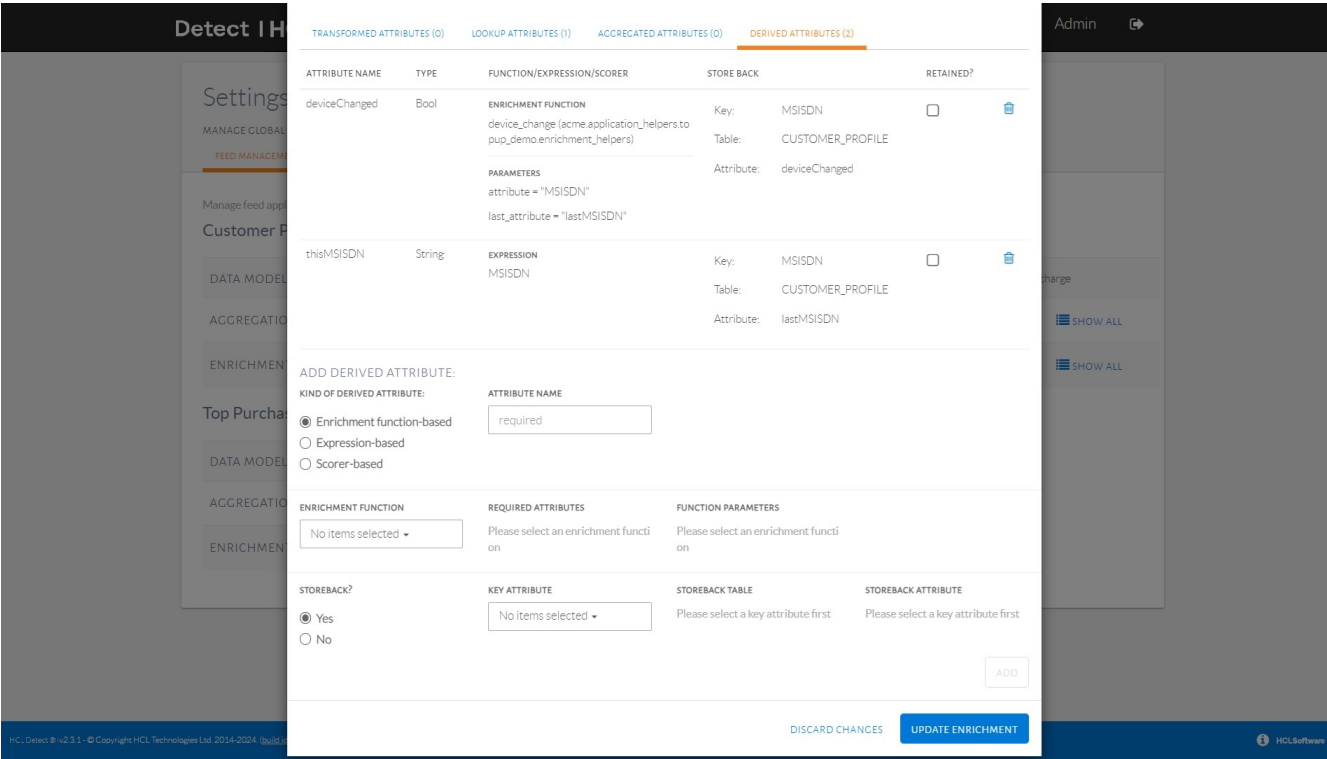
SELECT LOOKUP ATTRIBUTES: Please select a key attribute first INCLUDE

Please select attributes to be looked up

DISCARD CHANGES UPDATE ENRICHMENT

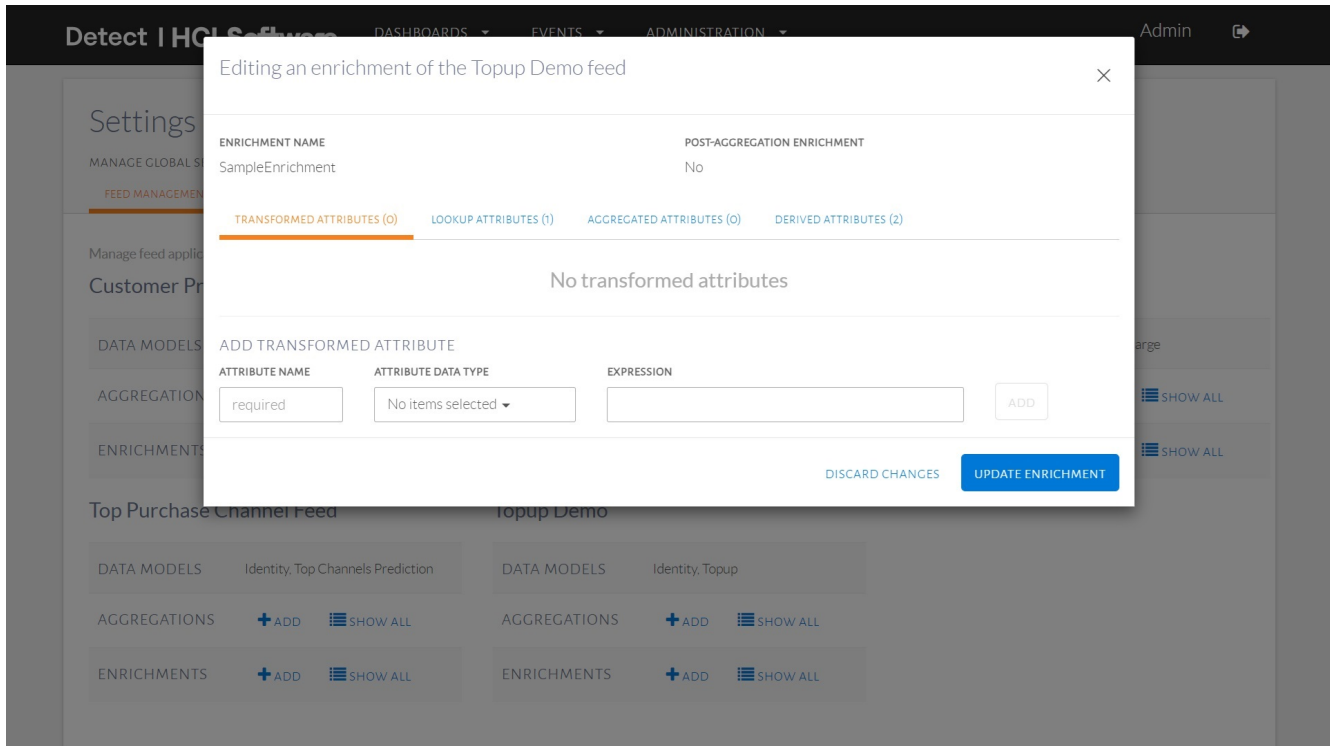
Interface for editing enrichments.

The interface for editing derived attribute type enrichments is shown below:



Interface for editing derived attribute type enrichments.

Enrichment operations can be configured to before aggregations are performed or after aggregations are performed. The value of a enriched *aggregate-based* attribute may change based on whether it configured to run before or after the aggregation operation. We can choose this while creating an enrichment by checking the **Post-Aggregation Enrichment** check-bit as shown in the below image:



Interface for creating a new enrichment.

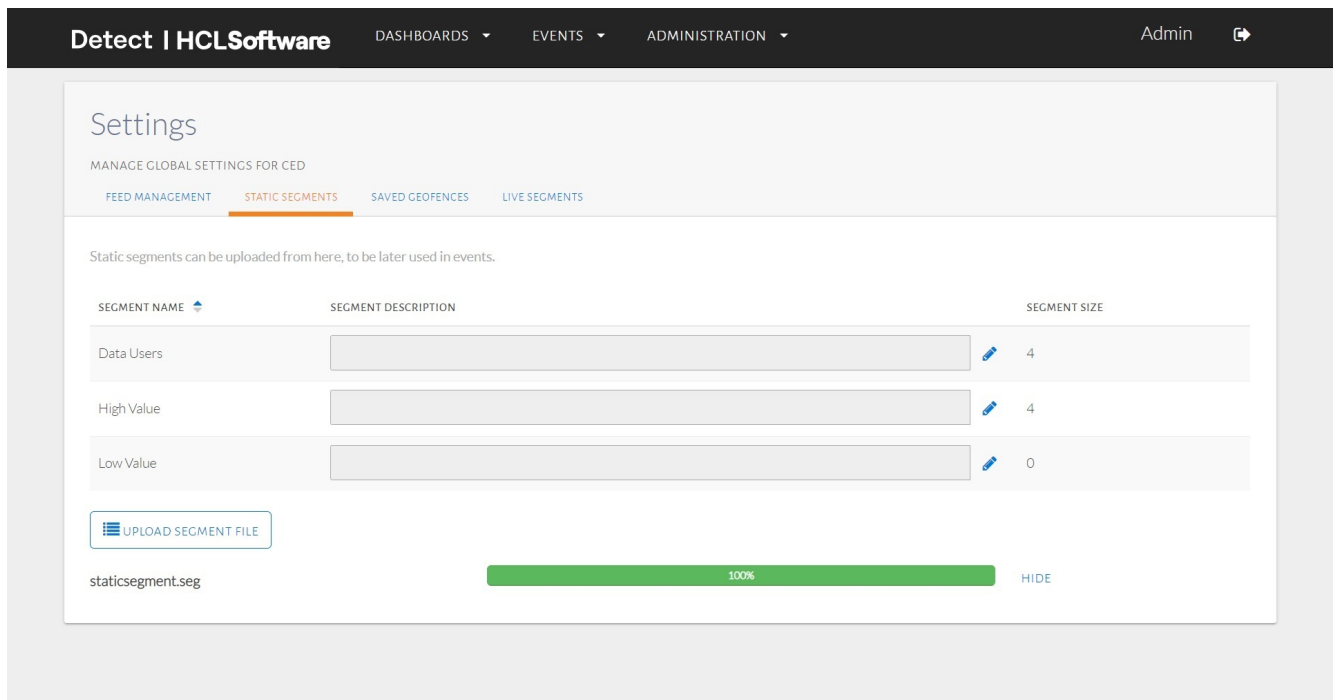
Chapter 5. Subscriber Segments

Segments are groups of customers with some similarities, setup segments based on preset conditions (Live), or through user selection list (Static). Grouping customers into Segments helps target them more appropriately or continuously across events with Detect. Detect supports 2 types of segments, Live & Static HCL Detect can make use of *subscriber segments*. Such segments can be used to include or exclude a group of subscribers from being considered as subjects for a trigger.

Static Segments

The set of `StaticSegments` can be inspected by clicking on `Settings` from the `Administration` menu and then selecting the tab titled `Static Segments`.

The example below shows a view of the page with 2 segments: the `DataUsers` and the `High Value` users.



Uploading a segment file.

To add, edit or delete a segment, a text file with its contents specified in a particular format can be uploaded to HCL Detect using the `UploadSegmentFile` button.

Two formats are supported. The first is a plain-text file with a simple linear organization as shown below:

```
[Data Users]: add
911323232323
918787879988
918787989021
919898990906
[High Value]: add
912323989899
912367367676
```

```

912398982337
919828738787
[High Value]: remove
912388728787
[Low Value]: remove_all

```

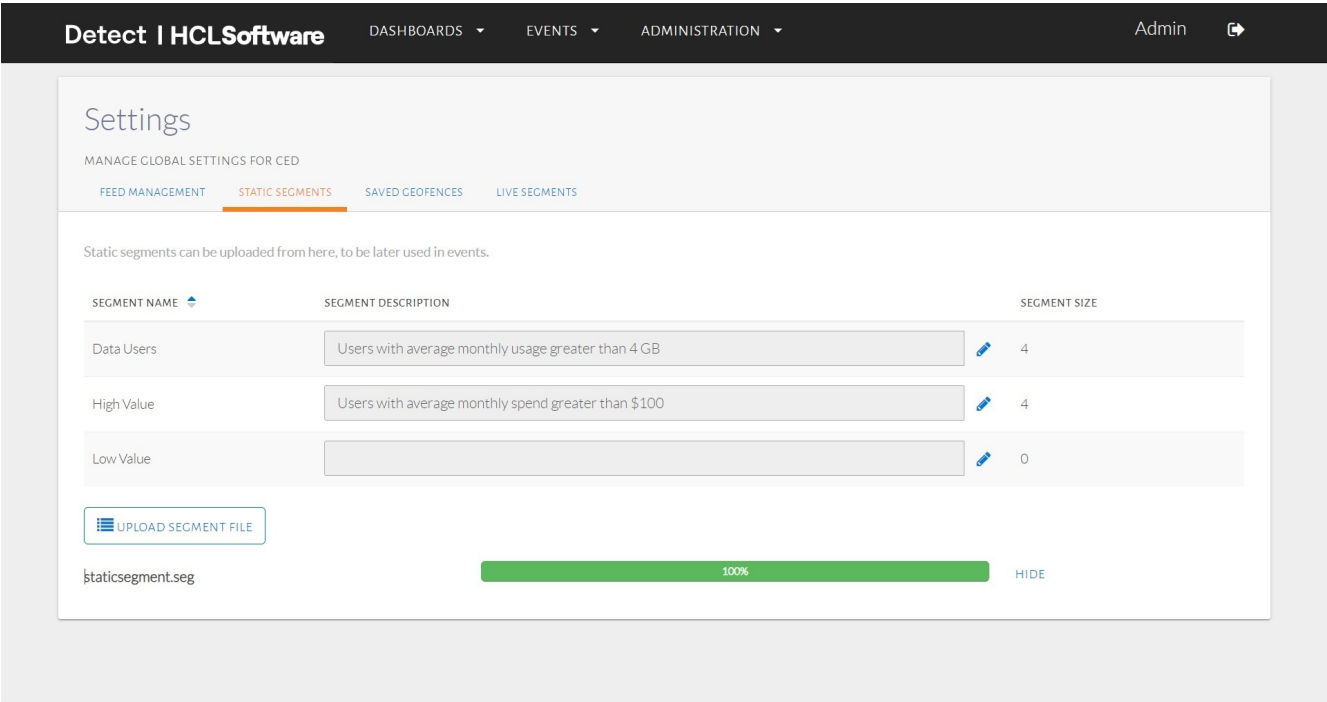
Alternatively, the file can also be specified in JSON format, in which case it must have a `.json` extension. An example is given below (note that the order of the fields is important):

```

{
  "segmentUploads": [
    {
      "operation": "Add",
      "segment": "Data Users",
      "users": [
        "911323232323",
        "918787879988",
        "918787989021",
        "919898990906"
      ]
    },
    {
      "operation": "Add",
      "segment": "High Value",
      "users": [
        "912323989899",
        "912367367676",
        "912398982337",
        "919828738787"
      ]
    },
    {
      "operation": "Remove",
      "segment": "High Value",
      "users": [
        "912388728787"
      ]
    },
    {
      "operation": "RemoveAll",
      "segment": "Low Value"
    }
  ]
}

```

Once uploaded, one can also add a description for the segments:



Segments and their descriptions.

Live Segments

Detect allows the user to enter a set of audience conditions and saves customers who meet those criteria in a Live Segment. Detect checks all customers against the defined conditions and maintains the segment over time. This means that Detect adds or removes customers from the segment as they fulfill or stop fulfilling the defined criteria. For example: if you'd like to frequently target customers who have the main balance atleast \$100 & who have installed a Mobile App i.e., Facebook, this can be saved as a Live Segment.

Detect will check all customers against the defined Main balance check & app installation status and sort the appropriate customers to the segment. Conditions can be setup as shown below:

Detect | HCLSoftware
DASHBOARDS
EVENTS
ADMINISTRATION
Admin

Demo Event
Demo Event
CREATED BY
admin
PROJECT
Demo
STATUS
DRAFT

Audience
Event Triggers
Events
Details
REVIEW AND SUBMIT FOR APPROVAL

Audience Criteria

All of the following:
Main balance amount
Subscribers who have the main balance at least \$ 100.00...
Installed mobile applications
Subscribers who have installed MobileApp1 mobile application(s)

EXCLUDED STATIC SEGMENTS
None

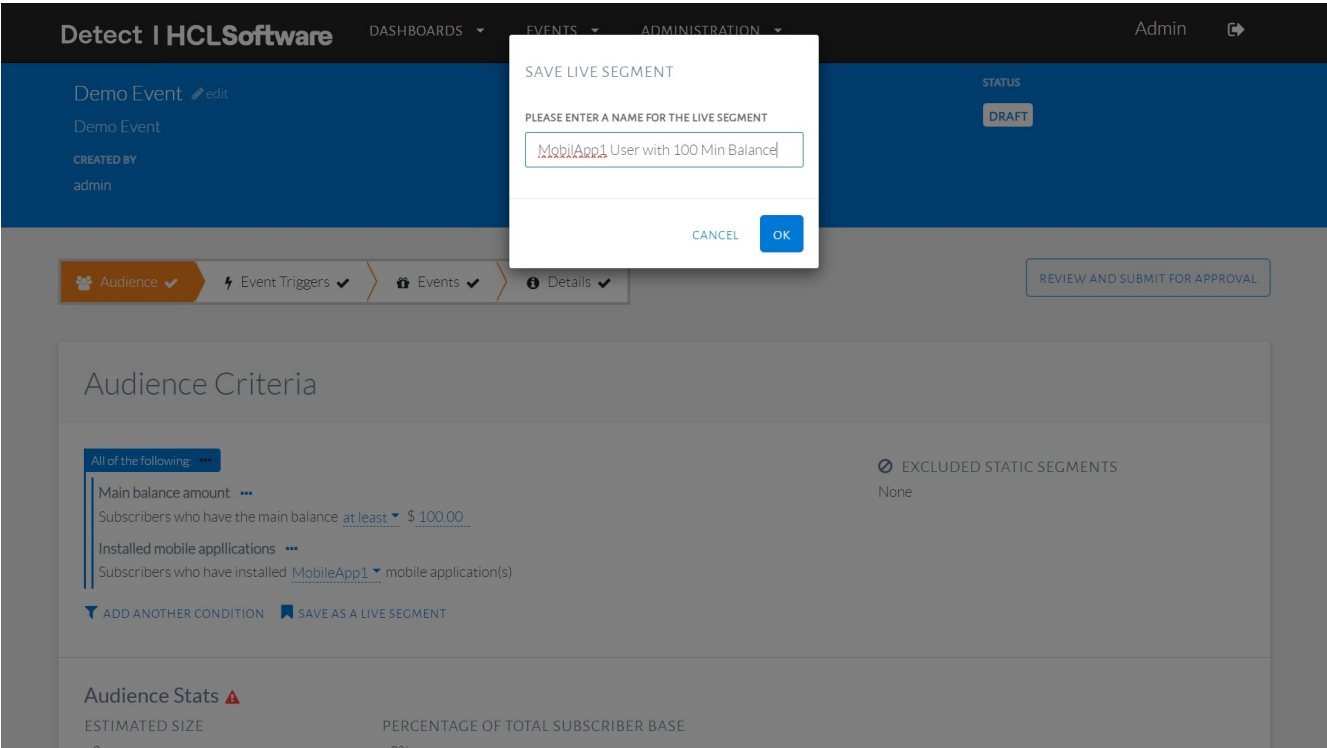
ADD ANOTHER CONDITION
SAVE AS A LIVE SEGMENT

Audience Stats

ESTIMATED SIZE	PERCENTAGE OF TOTAL SUBSCRIBER BASE

Creating an audience condition.

To save above audience condition as reusable live segment, we need to click on `SaveasLiveSegment` button. A dialog will open to get the name of the live segment:



Saving a live segment.

Once the live segment is saved, the condition will be wrapped as a live segments. This live segment can be replaced and edited by clicking three dots on the live segment shown:

Detect | HCLSoftware DASHBOARDS ▾ EVENTS ▾ ADMINISTRATION ▾ Admin

Demo Event [edit](#) PROJECT Demo STATUS DRAFT

CREATED BY admin

Audience ✓ Event Triggers ✓ Events ✓ Details ✓ REVIEW AND SUBMIT FOR APPROVAL

Audience Criteria

All of the following: ***

- Live segment ***
- MobilApp1 User with 100 Min Balance

ADD ANOTHER CONDITION SAVE AS

SHOW CONDITIONS
REPLACE WITH CONDITIONS
REMOVE CONDITION

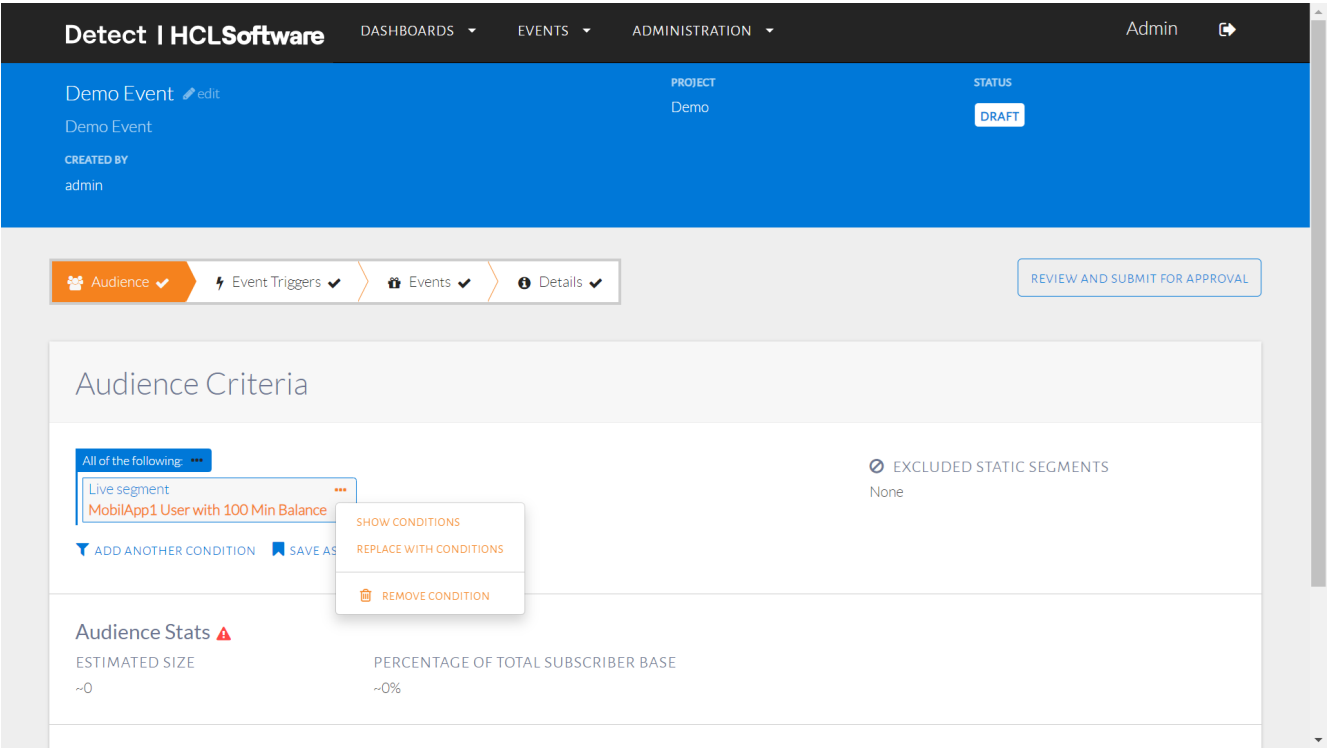
Audience Stats ⚠

ESTIMATED SIZE	PERCENTAGE OF TOTAL SUBSCRIBER BASE
~0	~0%

EXCLUDED STATIC SEGMENTS
None

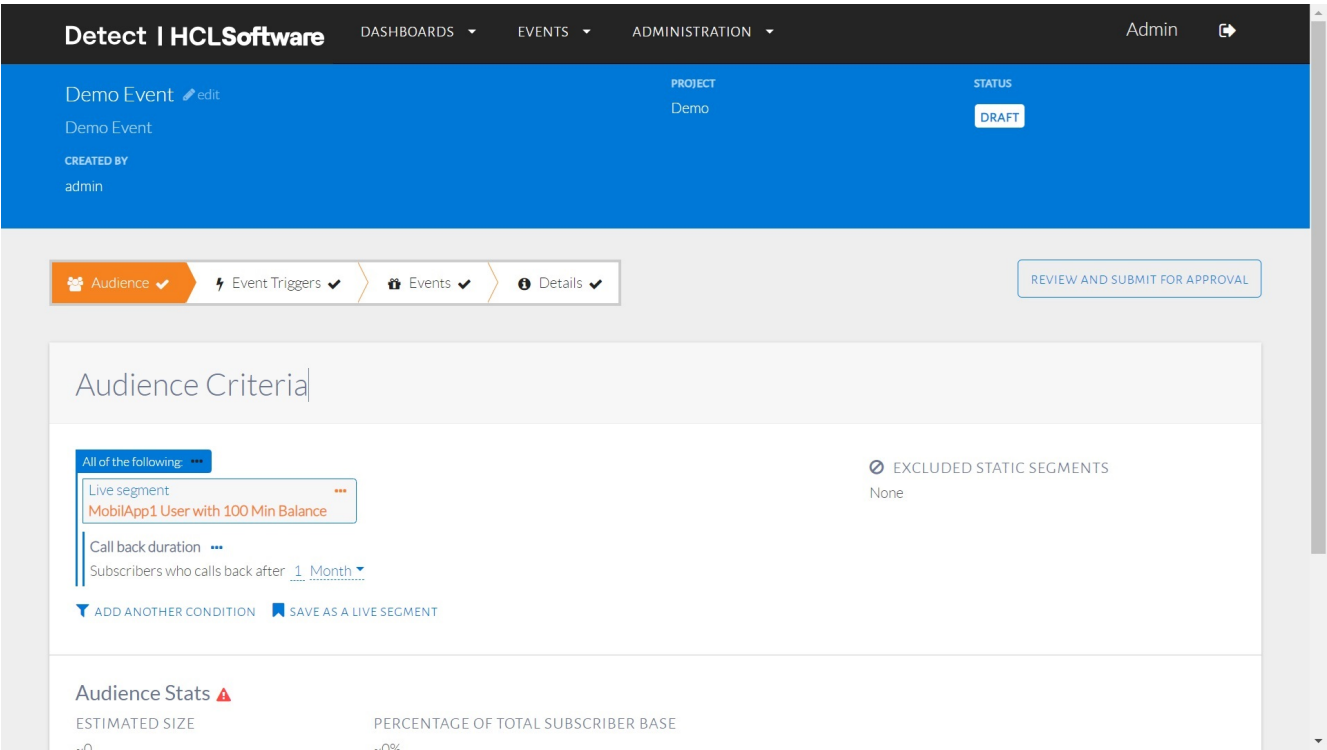
Using a live segment and editing it.

The set of `LiveSegments` can be inspected by clicking on `Settings` from the `Administration` menu and then selecting the tab titled `Live Segments`.



List of live segment.

Customers belonging to Live or Static Segments can be used as audience criteria by any user, in any event. Segments can be used along with other audience conditions as well, and can be added as shown below:



Audience condition using live segment and other audience conditions.