**Appthority User Portal: Functional Description**

Document Version: 1.0 (Draft)

**Document Control**

**Version History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version #** | **Author** | **Comments** |
| 2/26/2012 | 0.1 | [ssaxena@appthority.com](mailto:ssaxena@appthority.com) | Created the template |
| 03/06/2012 | 0.1 | [ssaxena@appthority.com](mailto:ssaxena@appthority.com) | Initial Draft with TBD functionalities |
|  |  |  |  |
|  |  |  |  |

**Approvals**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Approver Name** | **Project Role** | **Date** | **Signature/ Electronic Approval** |
|  |  |  |  |  |
|  |  |  |  |  |

**Table of Contents**

1. Introduction 4

2. As-is System Overview 5

3. Functional Description: User Portal 7

4. Login Page 8

4.1 User Authentication 8

4.2 Forgot Password 8

4.3 Request an Eval 10

4.4 Language Selection 10

4.5 Links 11

5. Dashboard 11

6. Header: Global Search 12

6.1 Global Search: App Link 12

6.1.1 Global Search: App Analysis 13

6.2 Global Search: All Result 13

6.3 Search Results 15

7. Header: Settings 16

7.1 Account Setting 17

7.2 MDM Setting 17

7.2.1 MDM Setting: MobileIron 18

7.2.2 MDM Setting: AirWatch 19

7.2.3 Settings: API Documentation 20

7.2.4 Settings: CDN Documentation 20

8. My Apps 21

8.1.1 Manage Apps: Submit Names or URLs 22

8.1.2 Manage Apps: Manual Upload 23

8.1.3 Manage Apps: Explore Public 23

8.1.4 Manage Apps: Import CSV 24

9. Explore 25

10. User and Groups 26

11. My Policy 26

11.1 Define Policy 27

11.2 Remediate 28

11.2.1 Remediate Actions 28

11.3 Global App Whitelist 29

11.4 Global App Blacklist 30

11.5 EULA 31

12. Marketplace (TBD) 32

Glossary 33

# Introduction

Appthority User Portal is a web-based application that allows Enterprise Users to check the mobile App for compliance with Enterprise Policy.

The purpose of this document to provide high-level component and functional description of as-is Appthority User Portal along with high-level dependencies of other applications on the shared resources like database used by Appthority User Portal. This documentation will help audience of this document, Developers and QA, to understand the portal ecosystem and functionality.

This document will also capture functional changes required for the Search & Sort and refactor and/or enhancements requirements.

The document organization, in chapters, is as follows:

1. Introduction: This chapter
2. As-is system description
   1. Overview of the eco-system
   2. Functionality of the portal
   3. Interdependencies of applications
3. Sort Changes
   1. Overview/Objective of Change
   2. Scope of the change
   3. Dependencies Management

This is a LIVE document and will be enhanced to incrementally describe as-is system and modification /enhancement to functionality.

# As-is System Overview

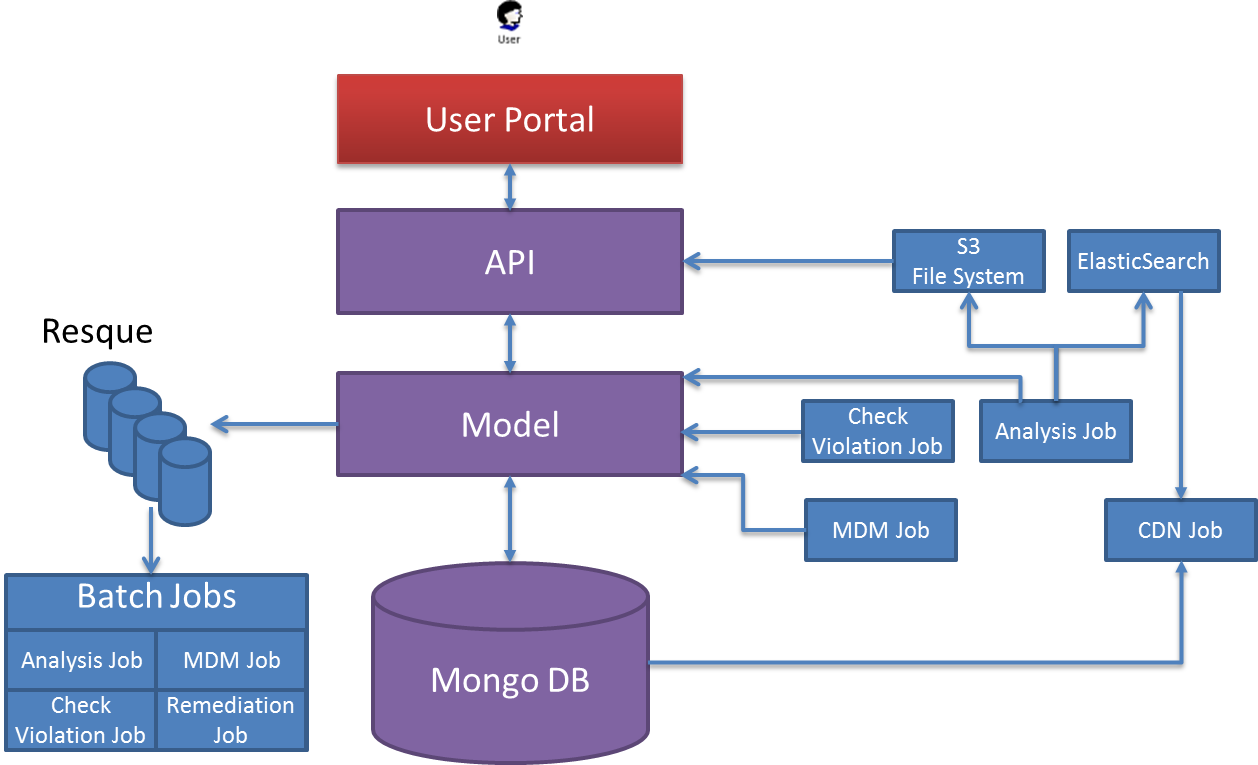


Figure 1: High-level components overview of the Appthority Portal Ecosystem

Figure 1, high-level components overview of the Appthority Portal Ecosystem depicts different components namely applications, middleware and databases that either interact with each other directly or have dependency on a shared resource. The components are as following:

* User Portal: Available to authorized Enterprise users, portals offers functionality to user to identify risk associated with their mobile App. User has access

1. Global Apps allowed by an Enterprise
2. Private App that user may download and install from marketplace outside the organization.

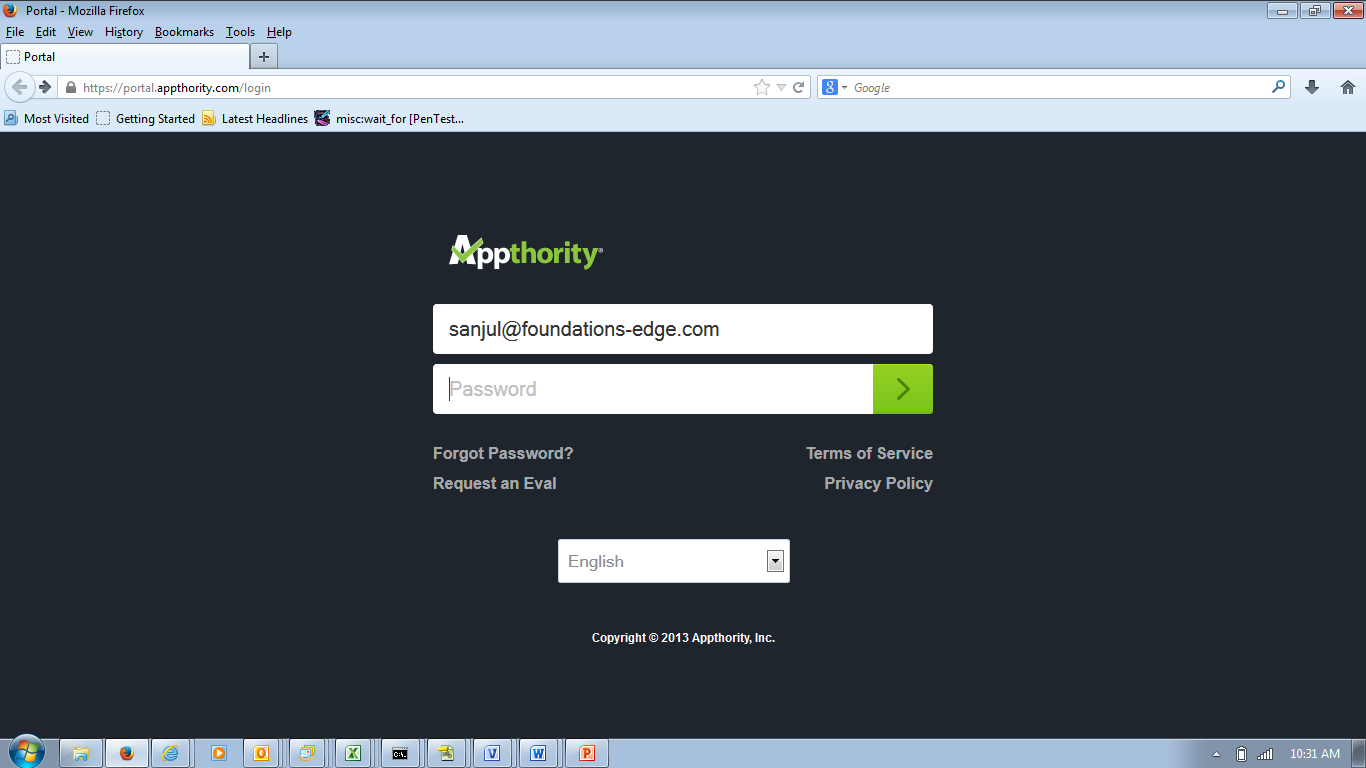
* Portal API: Portal APIs are deployed to support User Portal. All the user requests from the Portal are routed through Portal API. Portal API uses data model layer to service the user request.
* Model: Model is the abstraction of underlying database and provides uniform mechanism to access the database.
* Resque: Resque are populated by Model and hold the data for Analytics jobs
* Analytics Jobs: Analytics Job is responsible for processing the request from user to analyze the application. It pulls the data from Queue to process the job. After processing the App, Analytics Job updates the database, search and S3 file system.
* CDN Jobs: CDN job pulls data from Database and updates the content delivery system for improving the response for global users (non-US users)
* MDM Job: Description MDM job is responsible for connecting to the users MDM (example: MobileIron, AirWatch) and update the database with users MDM configuration like user and groups, devices etc.

# Functional Description: User Portal

User portal offers following functionality to the users:

1. Login: A username, password login screen for user to authenticates credentials and login to the portal.
2. Dashboard: Dashboard allows user to access different functionalities per the user authorization. Currently it offers following functionalities:
   1. Global Search: Allows user to search Apps and review App’s security attributes.
   2. My Apps: Allows user to review security attributes of Apps that are available in global and private repository.
   3. Explore: Explore is App explorer for all the Apps for different mobile platforms that are available in the system.
   4. User And Groups
   5. My Policy: This functionality allows user view and change security policy for evaluating Apps.
   6. Marketplace (Not Implemented)
   7. Settings: Settings allow user to configure setting associated with Mobile Device Management (MDM) applications and the account. User can also select logout over here to logout from the portal.
   8. Links: Portal provides helpful links to the user for following:
      1. Support: This link navigates to the Zen Desk support portal.
      2. Contact us: This link navigates to the Appthority Home page.
      3. Privacy Policy: This link displays Privacy Policy of Appthority to the user.
      4. Logout: Allows user to logout from Appthority portal.

# Login Page



The login page offers following functionality

1. User Authentication
2. Forgot Password
3. Request an Eval
4. Language Selection
5. Links
   * Terms of Service
   * Privacy Policy

## User Authentication

User email and password based authentication. Steps:

* User enter email address and password in text boxes
* User clicks on right Arrow or hits enter
  + User is Authenticated and dashboard page is displayed
    - Or
  + User error message is displayed

## Forgot Password

Email based password change request. Steps:

* Password recovery page is displayed
* User enters email-id
* Email with Link to change the password is sent to the user to reset the password
* User clicks on the link received in the email
* User is displayed “Change Your Password” page
* User enters the password and confirms it
* Clicking on “Change My Password” updates the password and takes user to login page
* Links
  + Sign In: Takes user to login page
  + Didn’t receive confirmation instruction?
    - Comes up with Blank Page
  + Terms of Service: Link to Terms of Service on Appthority site.
  + Privacy Policy: Link to Privacy Policy on Appthority site.

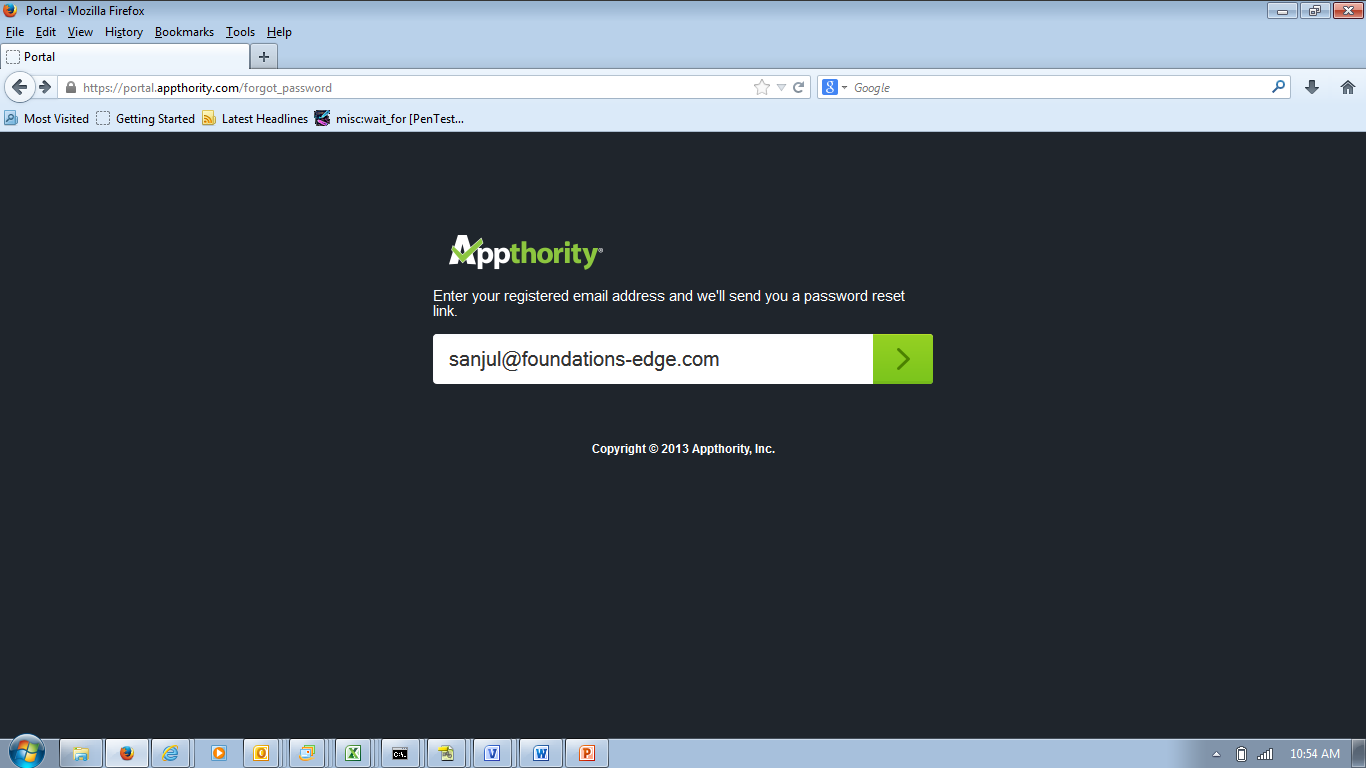


Figure 2: Password Change

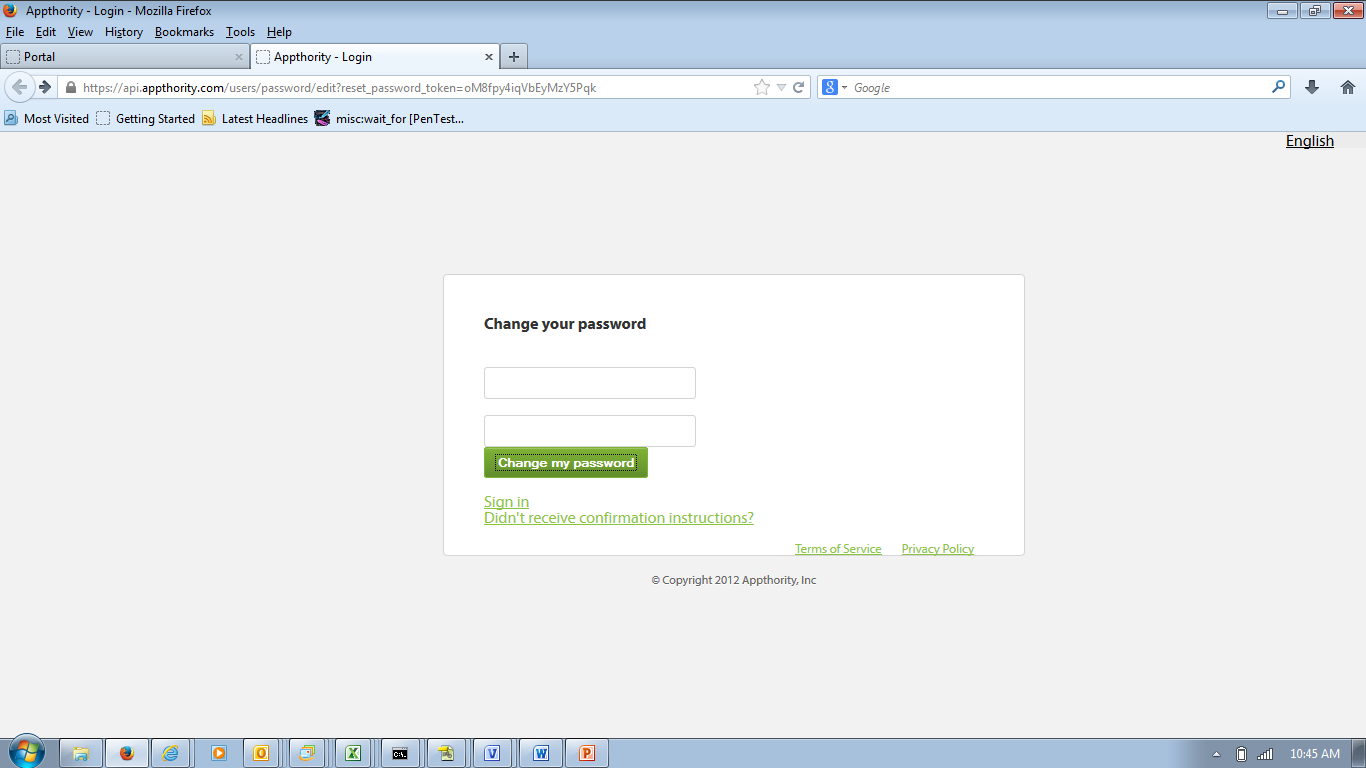


Figure 3: “Change Your Password”

## Request an Eval

This functionality is not supported by portal and will not require any enhancement.

~~This functionality allows user to request evaluation of Appthority service. Steps~~

* ~~Clicking on “Request an Eval” link on the login page brings up the Evaluation request form.~~
* ~~The user inputs First Name, Last Name, Company Name, Industry Vertical of the User/Company, Job Role of the user, Phone, Country, State, email address of the user, Password for the account and Checkbox for Terms and Conditions in the form: All fields are mandatory and has to be filled.~~
* ~~Clicking on “Submit Query” submits the form and displays the Appthority Home Page~~

~~TBC~~

## Language Selection

This functionality allows user to select language. Steps:

* User selects the language at the time of login.
* On successful authentication, user is asked to confirm the language if it has changed.
* On user confirmation, user views all pages in selected language.

## Links

Following are links to Appthority site and are not features of portal.

* + Terms of Service
  + Privacy Policy

# Dashboard

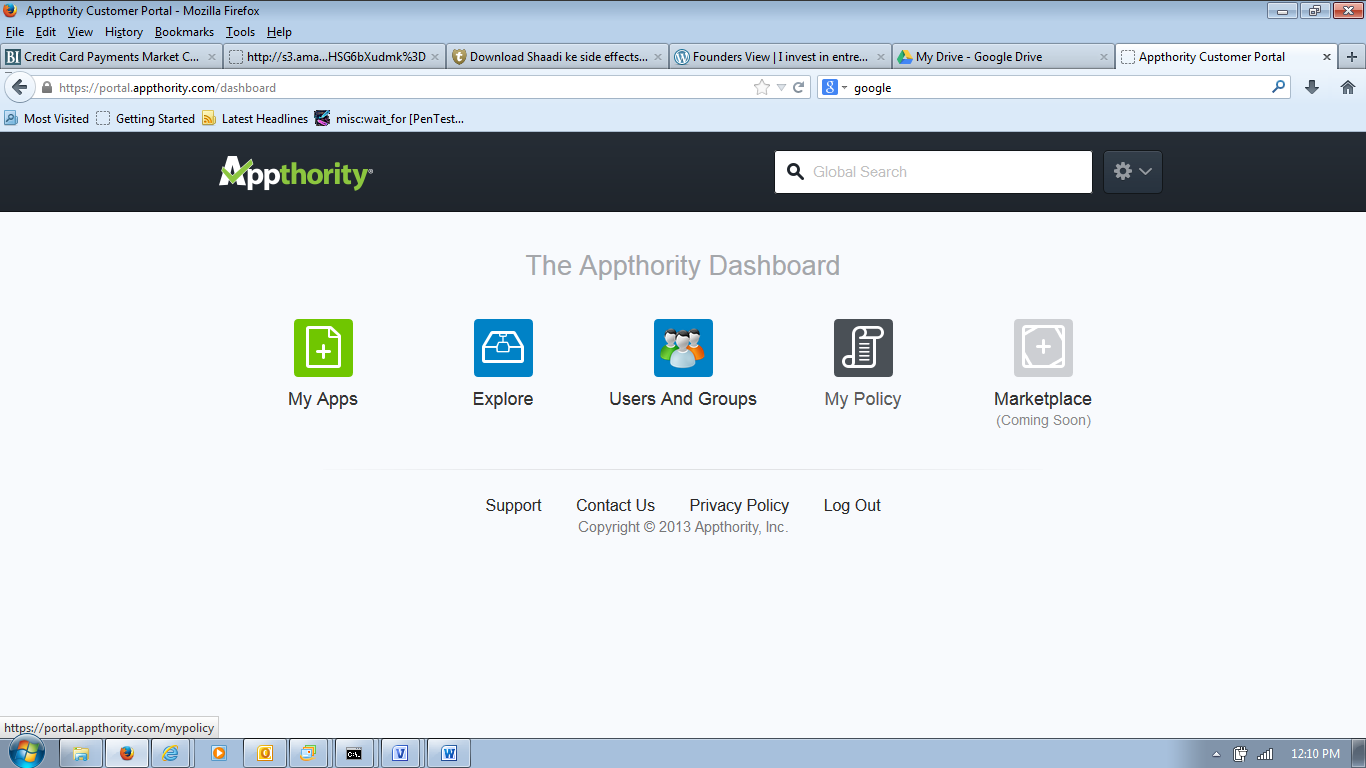


Figure: Dashboard

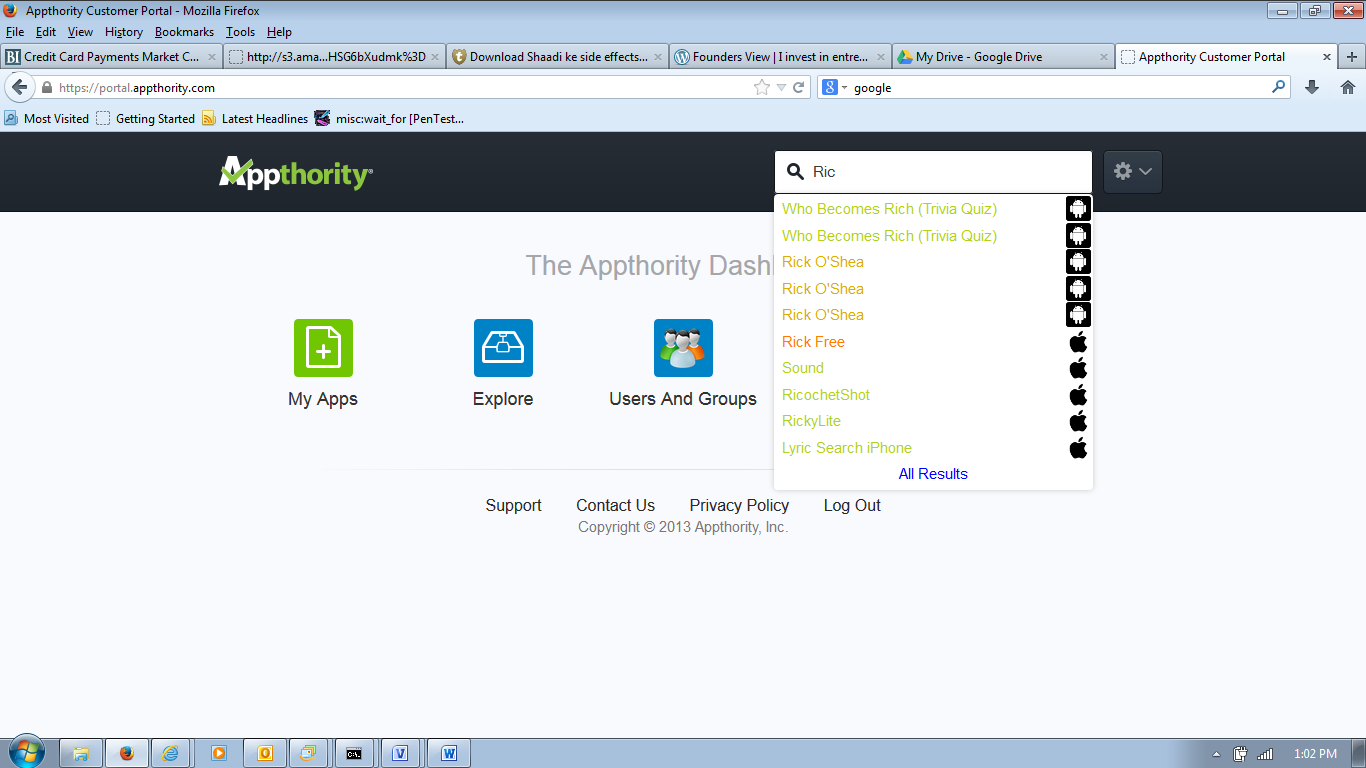
Dashboard is the main landing page after user login. It provides access in user-preferred language to following functionality

* Header: Header appears on all the pages and contains following functionality:
  + Global Search: Allows user to search for app.
  + Settings: Allows user to access MDM Settings, Account Setting and Logout.
* My Apps: Provides access to Public and Private mobile apps of the user and apps management feature.
* Explore: Allows user to explore the popular and top apps that are available on android and iOS for user to review.
* Users and Groups: Allows user to view users, devices and groups that are created in MDM.
* My Policy: Allows user to set the policy to evaluate the mobile apps.
* Marketplace (Coming Soon): This feature is not implemented.
* Footer: Footer appears on all the pages and contains links to following pages:
  + Support
  + Contacts Us
  + Privacy Policy
  + Logout

# Header: Global Search

Global Search allows user to search for the apps for android and iOS and display them to the user. Steps:

1. User types in characters of the App name to be searched
   1. There is no action for first two characters.
   2. On typing third letter: Drop-down appears with App recommendations, for both android and iOS with links to Apps and All Results.



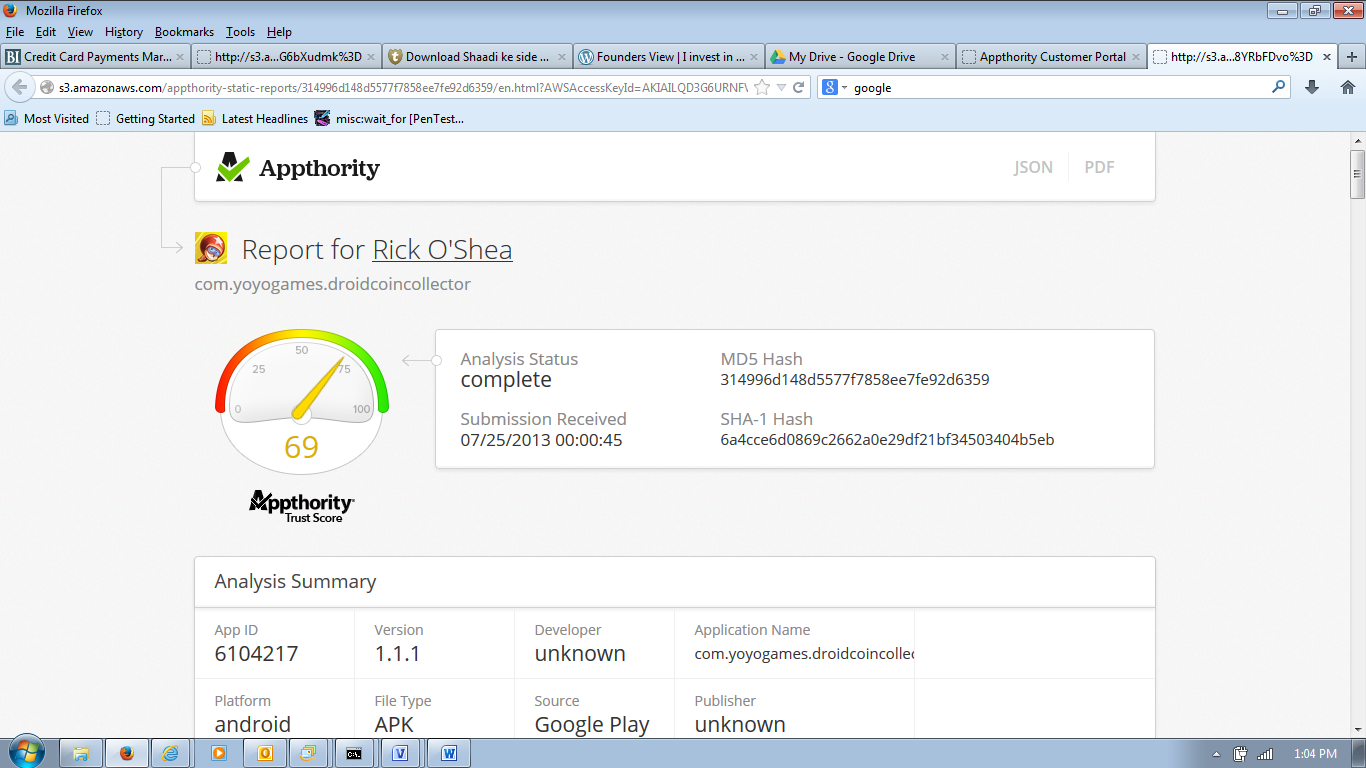
1. Clicking on the App name in the drop down displays App Analysis
2. Clicking on All result displays summary result for all the Apps.

## Global Search: App Link

Clicking on App Link in the search drop-down displays the App Analysis in a new window with two links

* JSON: Clicking on JSON link display the analysis information as a JSON strings
* PDF: Clicking on PDF link displays the analysis information as a PDF file that a user can save.

### Global Search: App Analysis



Analysis Report: Analysis report contains following information:

* High Level Trust Summary: Trust summary contains of App Trust Score, MD5 Hash, Submission Received, SHA-1 Hash.
* App Summary: Analysis Summary contains, App Identifier, Version of the App, App Name, Platform of the App etc.
* Behavioral Details: Following behaviors of the App’s are captured:
  + Risky Behaviors
  + Privacy Behaviors
  + Hostname, IPS and URLS accessed by the App
  + Emails used by the App.

## Global Search: All Result

Clicking on All Result in the global search display summary of each App found for Android and iOS using the search term. No results are displayed when two or less characters are typed in the Global Search box.

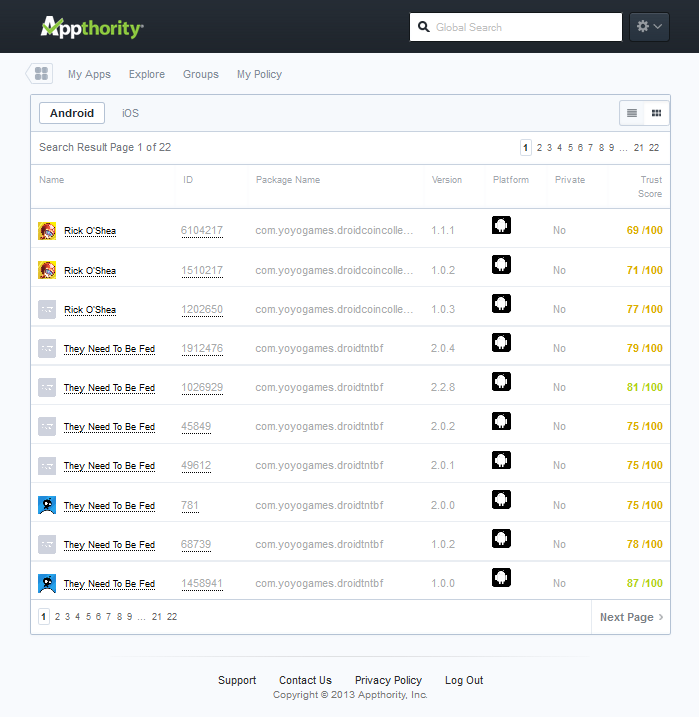


Figure: Global Search List Display

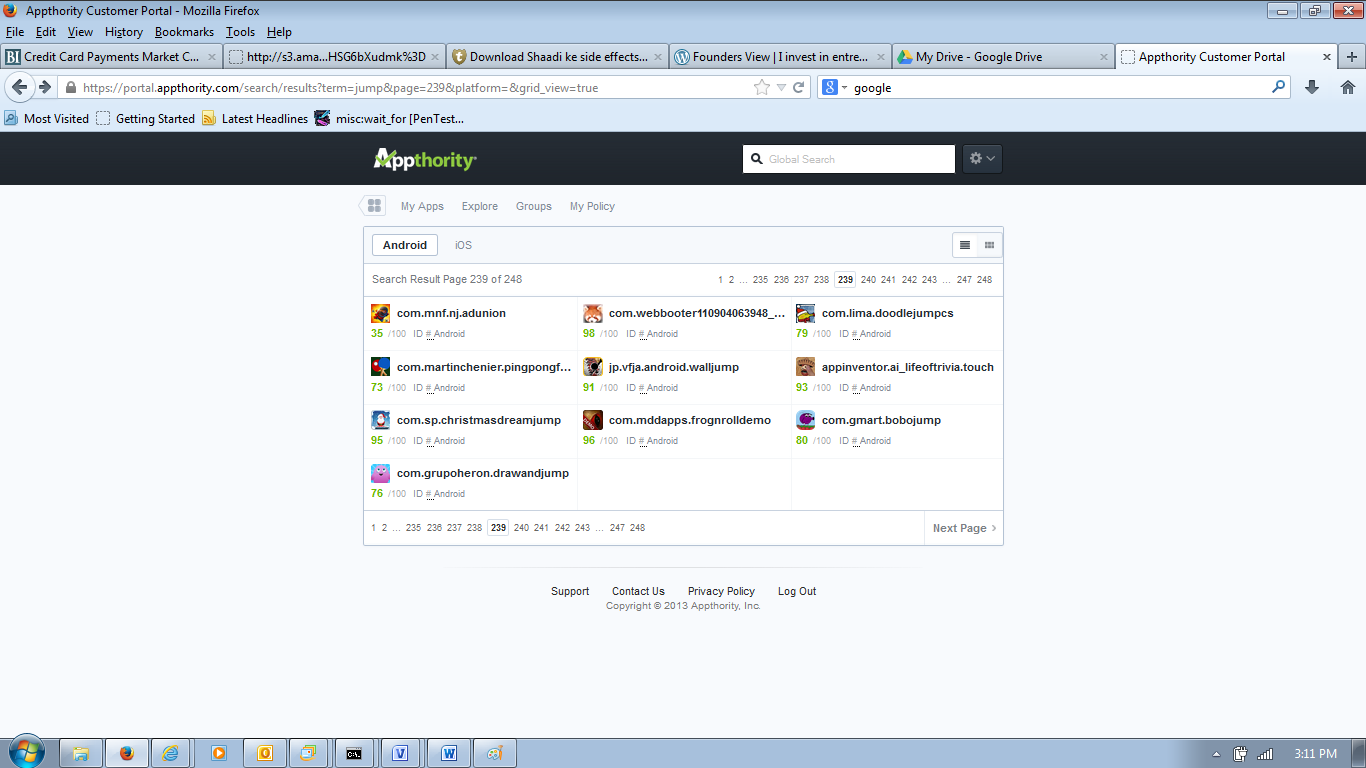


Figure: Global Search Grid Display

“All Result” page contains following functionality:

* Header: Header functionality is described in Chapter 5, 6 and 7
* Navigation Menu: Navigation Menu contains following functionality
  + Icon to access dashboard
  + Links for My App, Explore, Groups and My Policy
* Search Results: Results of the search grouped by Android and iOS
* Footer

## Search Results

Search Results displays all the Apps that are found using the search term. The functionality of the page is as following:

* Displays all the Apps that are found using the search term
  + Search API’s uses Elastic Search
* The results are grouped by Android or iOS
* By default all the Apps for Android are displayed
* Clicking on iOS display the Apps that are found for the iOS
* 10 results are displayed per page
* By default results are displayed as list
* Results can be displayed as grid of icons
* Page navigation: All the Apps found using the search term are organized in pages
  + All the Apps with same name are grouped together
  + Maximum 13 links are displayed
    - Link to first two pages
    - Link to 9 continuous search result pages depending on user.
      * For first time 9 links are continuous from 1 to 9
      * If user clicks towards end – 9 links are continuous through to the end
      * If user clicks in between the page is centered in the link (5th in the order)
    - Link to last two pages
* Result information
  + Name of the app
  + ID of the app
  + Package name of the app
  + Version of the app
  + Platform of the app
  + Flag indicating if the app is private or not
  + Trust score of the app.

Clicking on the name or id of the app displays the App Analysis (See section 6.1.1).

NB: Actual ID # is not displayed in the Grid View. Clicking on the ID # displays the App Analysis.

# Header: Settings

Selecting Account Setting or MDM Setting from Setting dropdown in the header of the page provides following functionality:

* Header: Header functionality is described in Chapter 5, 6 and 7
* Navigation Menu: Navigation Menu contains following functionality
  + Icon to access dashboard
  + Links for My App, Explore, Groups and My Policy
* Setting Page: Setting page provides following functionality
  + Left Navigation Bar: Provides access to Account Setting, MDM Setting, API Documentation, and CDN Documentation. Account Setting or MDM Setting page is opened depending on the user selection in Setting’s dropdown.
* Footer Links

## Account Setting

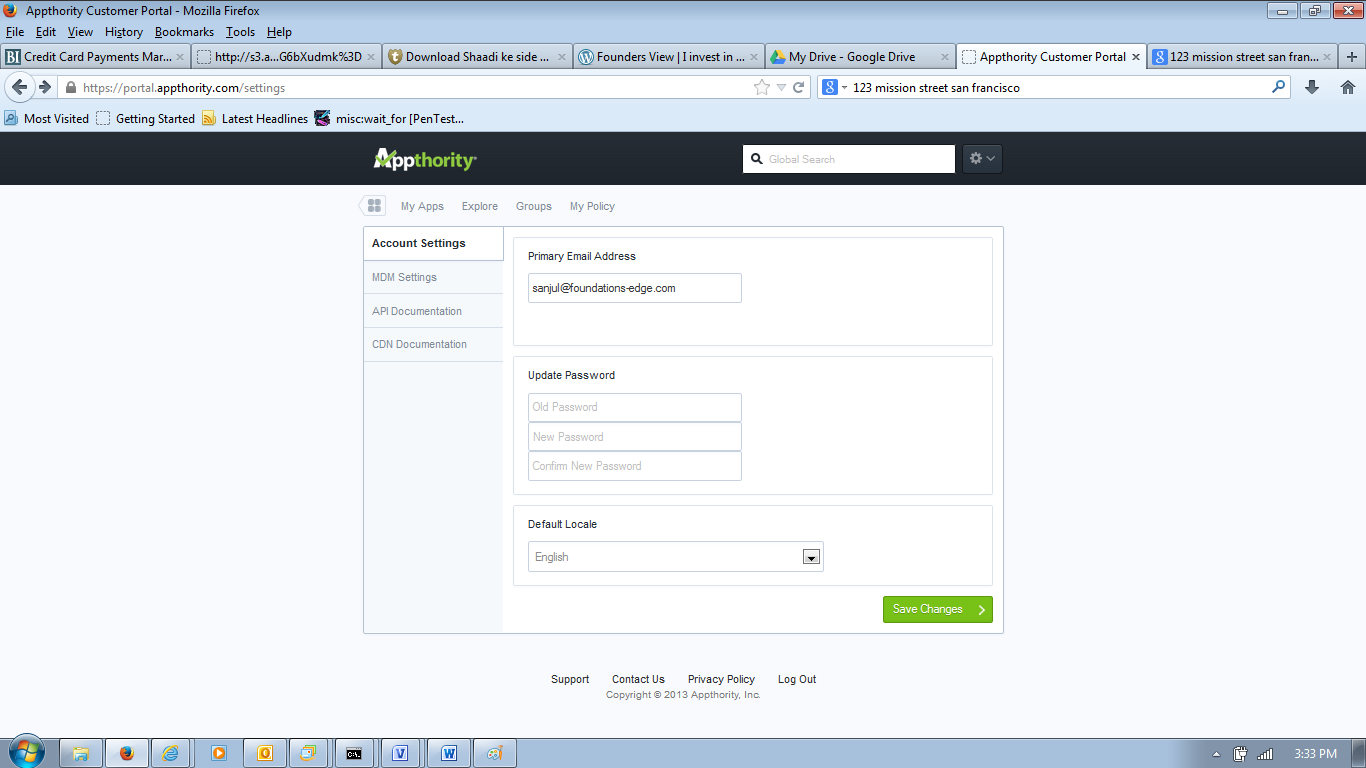


Figure: Account Setting Page

Account Setting Page offers following functionality to the user:

* Primary Email Display: User cannot change the primary email address.
* Update Password: Update password allows user to change the current password with a new password.
* Default Locale: Drop down containing languages that a user can select for using Appthority’s Portal.
* Save Changes: If modified by the user, clicking on Changes save the changes to Password and/or Locale.

## MDM Setting

MDM setting allows user set the MDM provider. Currently MobileIron and AirWatch are supported. User can select either from the MDM provider dropdown.

### MDM Setting: MobileIron

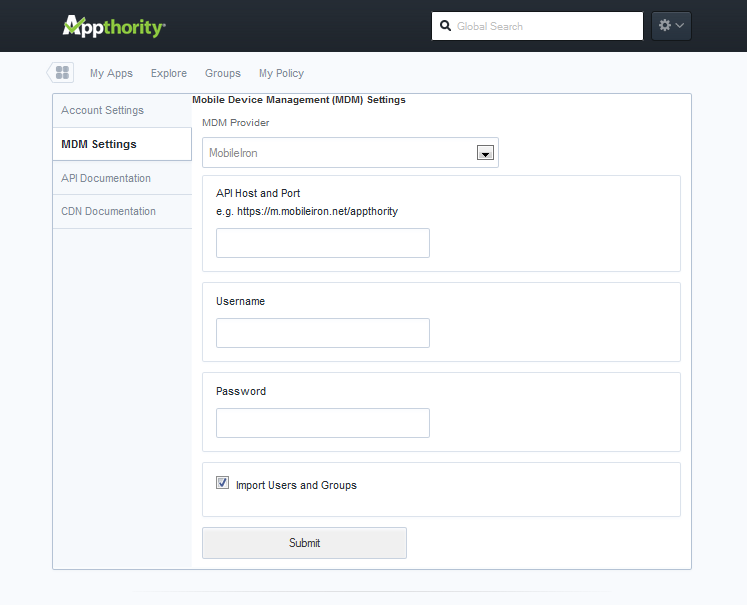


Figure: MDM Setting MobileIron

Figure, MDM setting MobileIron gives overview of the settings required for the MobileIron MDM. Functionality offered by the page are:

* Fields to input MobileIron MDM connection information: The required fields are:
* API Host and Port: Host and Port entry for the MobileIron MDM
* Username: Username to access MobileIron MDM
* Password: Password associated with Username
* Import Users and Groups: Checkbox to indicate if users and groups are to imported from the MDM.
* Submit button: Submit button will submit the information to Appthority Application.
  + User credentials for MDM is checked; if credentials fails then message is displayed
  + Message to pull data from MDM is sent to Resque

### MDM Setting: AirWatch

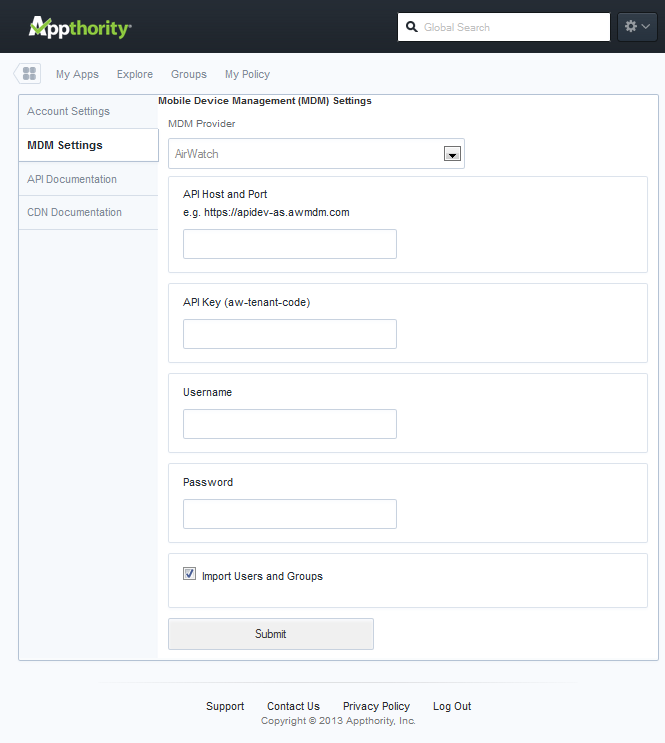


Figure: MDM setting Airwatch

Figure, MDM setting Airwatch gives overview of the settings required for the Airwatch MDM. Functionality offered by the page are:

* Fields to input Airwatch MDM connection information: The required fields are:
* API Host and Port: Host and Port entry for the Airwatch MDM
* API Key(aw-tenant-code): Key to access AirWatch MDM
* Username: Username to access AirWatch MDM
* Password: Password associated with Username
* Import Users and Groups: Checkbox to indicate if users and groups are to imported from the MDM.
* Submit button: Submit button will submit the information to Appthority Application.
* User credentials for MDM is checked; if credentials fails then message is displayed
* Message to pull data from MDM is sent to Resque

### Settings: API Documentation

Clicking on API Documentation displays the guidelines to integrate with Appthroity Rest API.

### Settings: CDN Documentation

Clicking on CDN Documentation displays the guidelines to integrate with CDN.

# My Apps

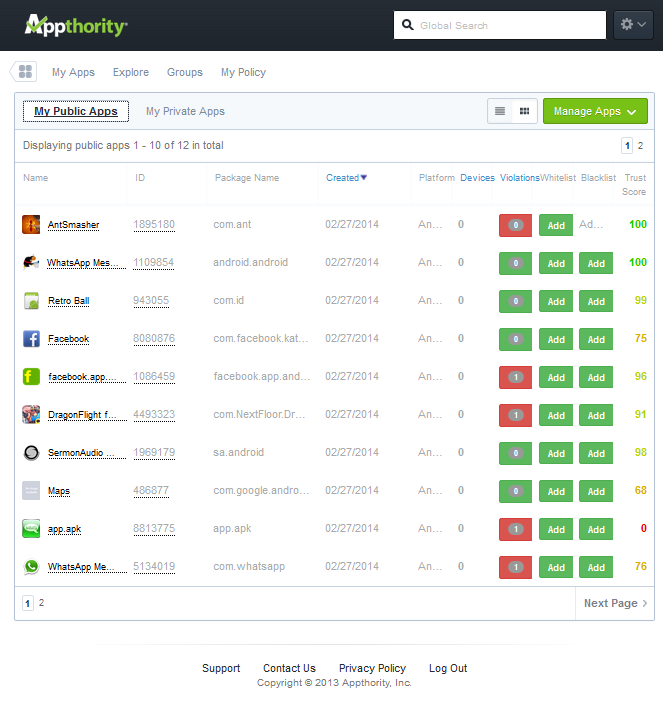


Figure: My Apps overview

Selecting My Apps from Dashboard or Clicking on My Apps in Menu displays the My Apps page with My Public Apps as default list of Apps.

My Apps offers following functionality:

* Header, Footer and Menu Navigation for Dashboard, Explore, Groups, and My Policy.
* Paginated list of My Public List (default list) with 10 apps per page.
  + Review APP report by clicking on App name or App Id
  + Review violations by clicking on violations
  + Add App to white list or black list (mutually exclusive)
  + Sort App list on Date Created, Devices, Violations,
  + Navigate through pages by clicking on page numbers.
  + View Trust Score of Apps.
* Option to switch between My Public Apps and My Private Apps
* Options to view Apps in grid view or list view
* Manage Apps to add new Apps
  + Submit Names or URL of App for generating analysis
    - Request to be queued
  + Manually Upload Apps from local system for analysis
    - Request to be queued
  + Explore Public Apps
  + Import multiple Apps for analysis via CSV file
    - Request to be queued

### Manage Apps: Submit Names or URLs

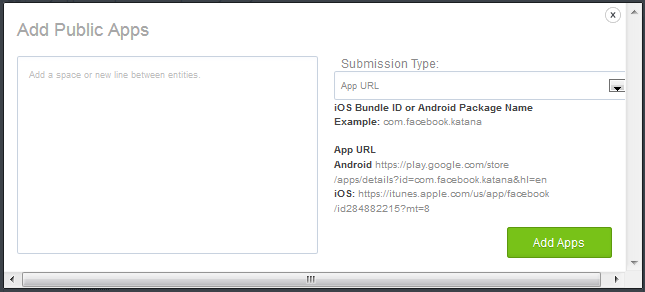


Figure: Submit Names or URLs overview

Allows user to submit names or URLs of the Apps for analysis and adding the analyzed apps to “My Public Apps”.

It offers following functionality:

* Text box to add names or URL of Apps; All the entries should be same type
* Dropdown to select submission type
* Add Apps button to submit the Apps

Message is queued for batch job to process the list of Apps submitted by user.

### Manage Apps: Manual Upload

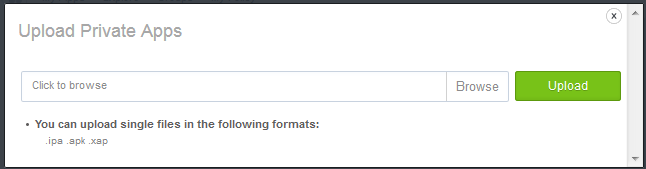


Figure: Upload Private Apps Overview

Allows user to submit Apps for analysis and adding the analyzed apps to “My Private Apps”.

It offers following functionality:

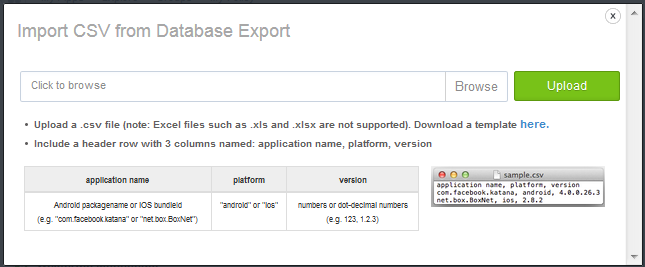
* Browse the local system for selecting an App
* Upload button to submit the App

Message is queued for batch job to process the App submitted by user.

### Manage Apps: Explore Public

This is same as link to Explore in Naviagtion Menu

### Manage Apps: Import CSV



Allows user to submit CSV file containing list of Apps for analysis and adding the analyzed apps to “My Public Apps”.

It offers following functionality:

* Browse the local system for selecting an CSV file containing list of Apps
* Upload button to submit the CSV file
* Download link for template CSV file to assist user in preparing the file

Message is queued for batch job to process the list of Apps submitted by user.

# Explore

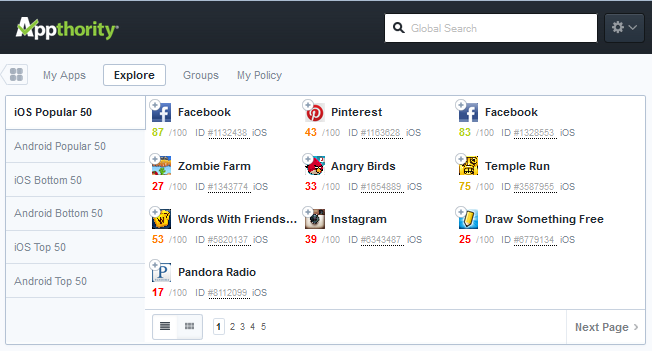


Figure: Explore Overview

Explore offers following functionality:

* Header, Footer and Menu Navigation for Dashboard, My Apps, Groups, and My Policy.
* Navigation to view Most Popular, Top and Bottom ranking Apps for iOS and Android.
* Paginated list of Public List with 10 apps per page.
  + Review App report by clicking on App name or App Id
  + Add App to My Public Apps by clicking on Add (+) icon on the App
  + Identify App if already in My Public Apps (Check icon instead of + icon)
  + Navigate through pages by clicking on page numbers or Next Page
  + View Trust Score of Apps.
* Options to view Apps in grid view or list view

# User and Groups

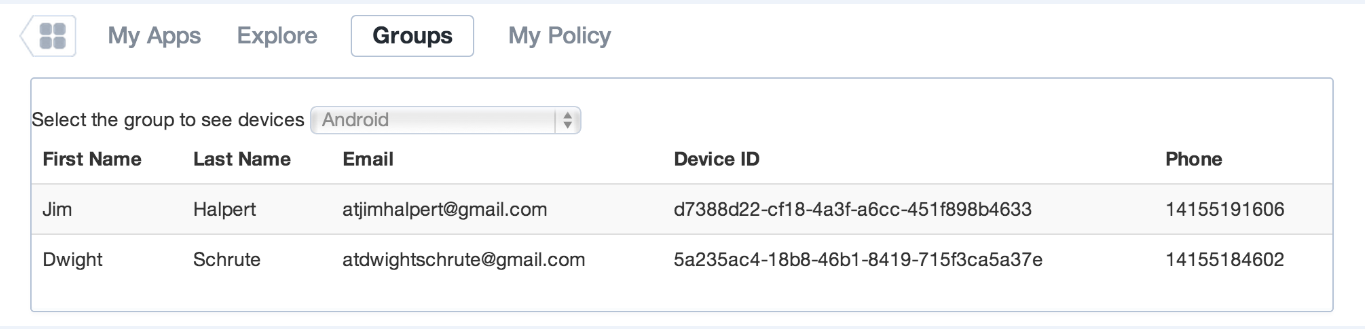


Figure: Groups Overview

Allows user to filter the devices by Groups and view them in portal. It offers following functionality:

* Filter to Select the group
* List of devices with following information
  + Name (First Name and Last Name) of Device User
  + Email id of the Device User
  + Id of device assigned to Device User
  + Phone number of the Device User
  + Page Navigation to review the entire list.

Note: This information is pulled by a batch job from MDM and stored in DB. MDM is configured through settings menu.

# My Policy

My policy allows user to manage policies. It offers following functionality:

* Define Policy: Policy for group of devices. This is also the default landing page for “My Policy”
* Remediate: Take remedial action through MDM
* Global Whitelist: View and remove Apps for Global Whitelist
* Global Blacklist: View and remove Apps for Global Blacklist
* EULA: Manage EULA for Apps.

## Define Policy

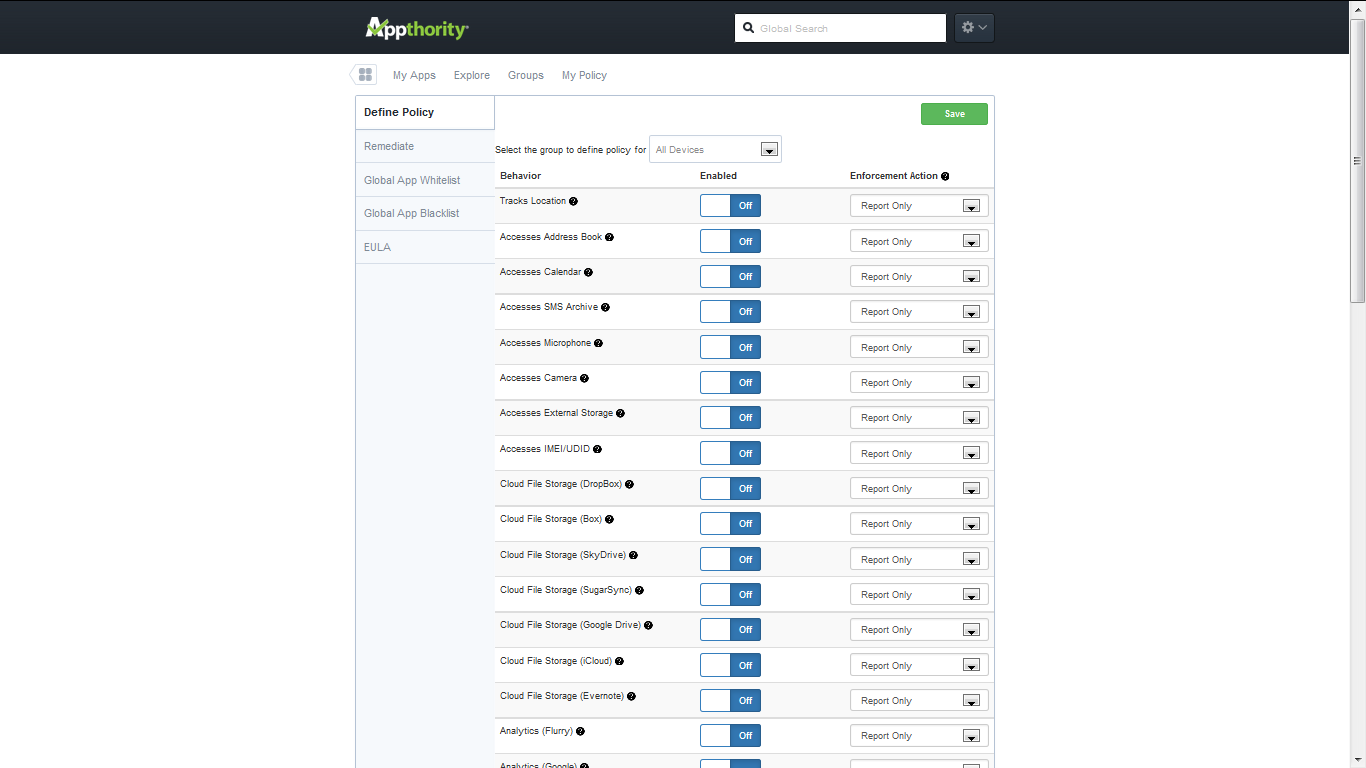


Figure: Overview of Define Policy

Define Policy page offers following functionality to the user:

* Select a group of devices to review the policy information – by default policy information applicable to All devices is displayed.
  + List all the behavioral elements for the selected group of devices
* Manage configuration of Behavioral elements by switching them off or on
  + Policy elements have binary value either On or Off
* Define Enforcement Action if Application does not comply with configuration of behavioral element
  + Actions supported are Send a report, Send a Message, Retire Device
* Button to Save the Changes to the policy
  + Queues job for violation check according to the modified policy.

## Remediate

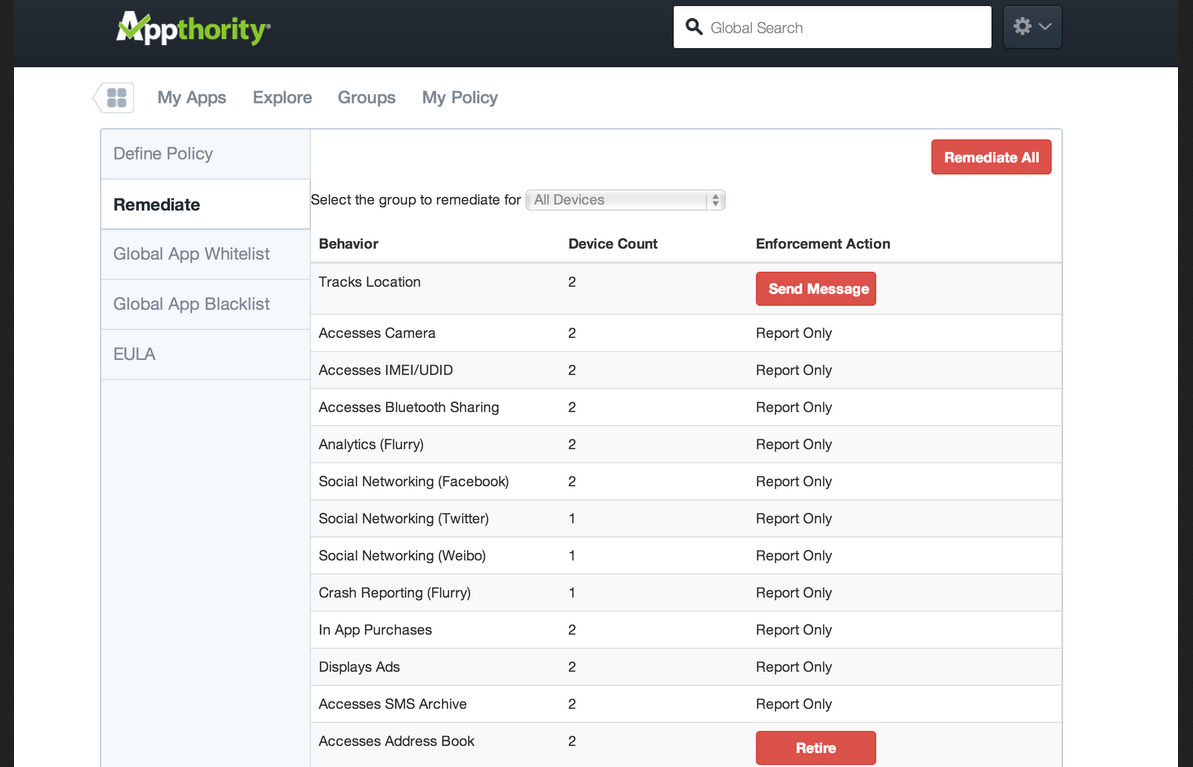


Figure: Remediate Overview

Remediate page allows user to take action against the devices that have apps violating the policy. It provides following functionality:

* List all the behaviors where apps on devices are violating the policy
  + Violated behavior
  + # of Device with Apps violating specific behavior
  + Selective enforcement action that user can apply for a violation
* Allows user to filter the devices by group
* Allows user to take remedial action for specific violation
  + Select action button against specific violation
  + Message is queued for remediation job
* Allows user to take remedial action for all violations.
  + Remediate All
  + Message is queued for remediation job

### Remediate Actions

Following remediation actions are allowed:

* Report Only: The devices that have Apps with specific behavior in violation will be reported/logged. No further action will be taken
* Send Message: The devices that have Apps with specific behavior in violation will be sent SMS message informing the user of the device about the violation. No further action will be taken.
* Retire: The devices that have Apps with specific behavior in violation are quarantined and message is sent to them.
* The action to Send Message and Retire are queued in Resque
  + Remediation job sends the action request to MDM.

## Global App Whitelist

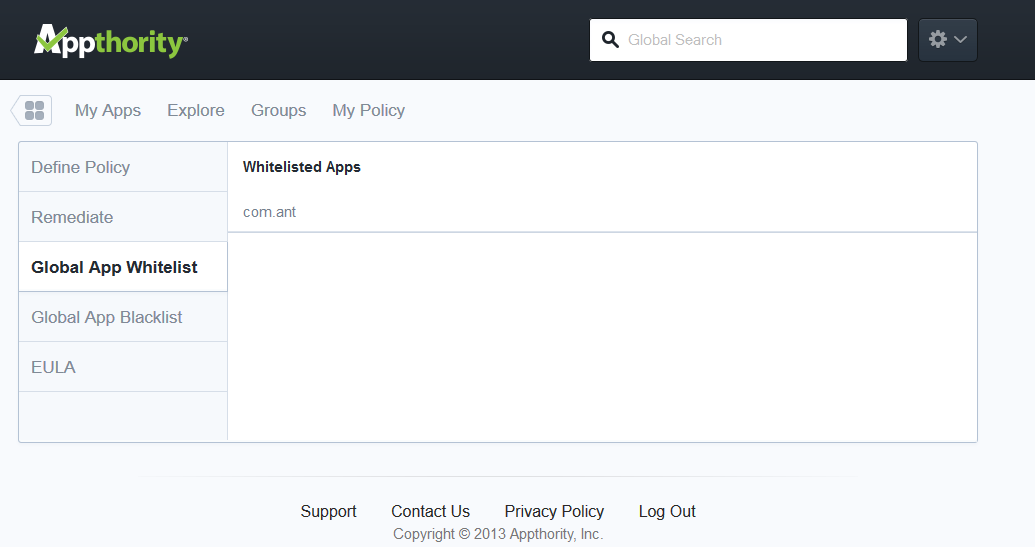


Figure: Overview of Global App Whitelist

Global App Whitelist lists all the Apps that are whitelisted by the user. The functionality offered is as follows:

* List all the Whitelisted Apps
* Remove App from Whitelist

## Global App Blacklist

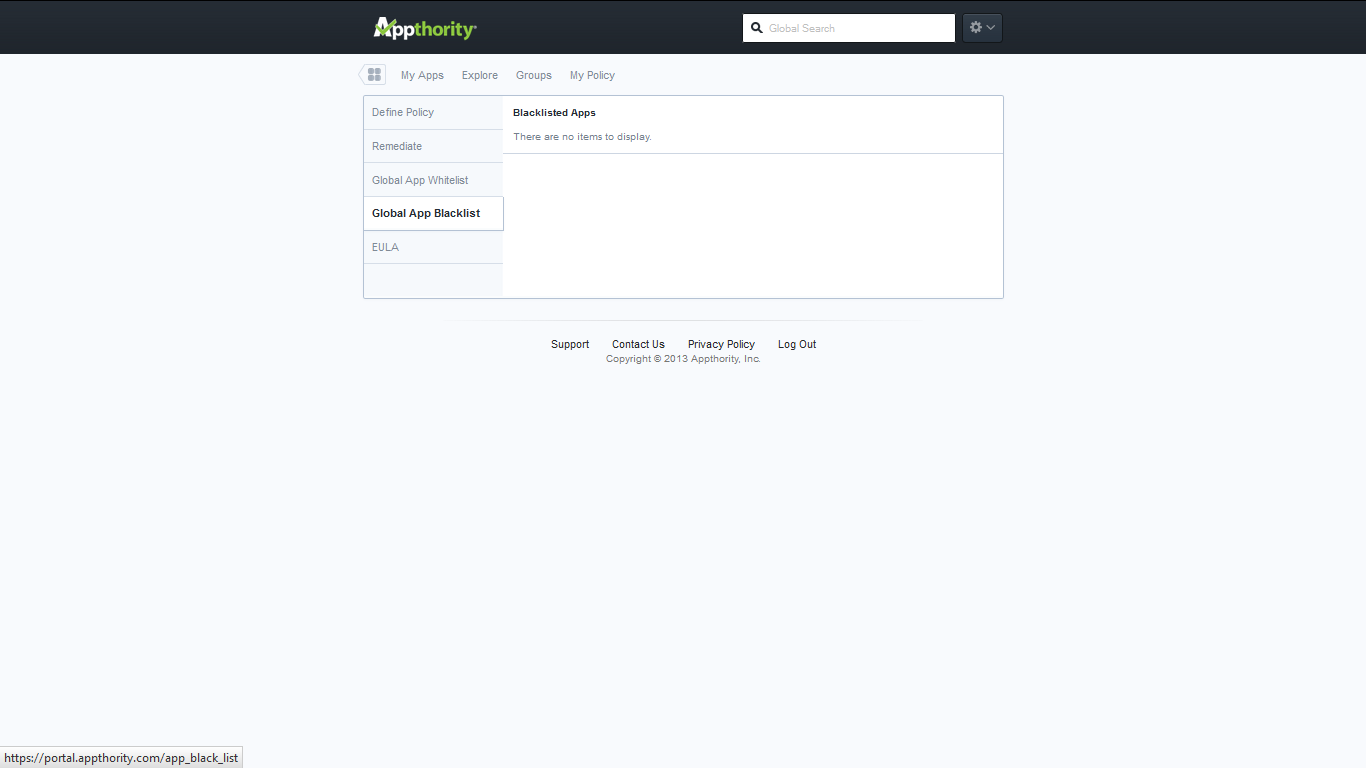


Figure: Global App Blacklist

Global App Blacklist lists all the Apps that are blacklisted by the user. The functionality offered is as follows:

* List all the Blacklisted Apps
* Remove App from Blacklist

## EULA

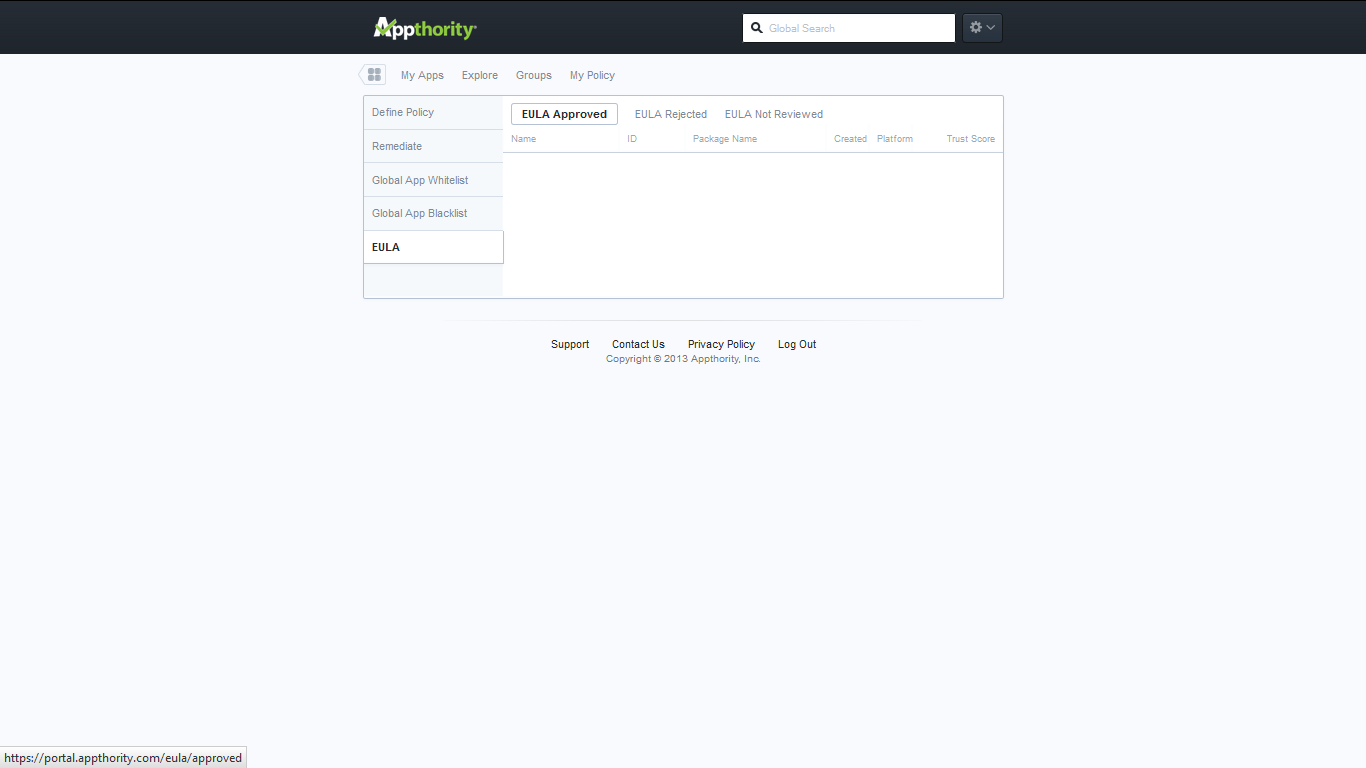


Figure: EULA list overview

EULA page allows user to review the approval status of EULA for the apps. It offers following functionality:

* List all the apps for which EULA is approved (Default view)
* List all the apps for which EULA is rejected
* List all the apps for which EULA is not reviewed

Following information is displayed for the Apps with EULA Approved/Rejected:

* Name of the Application
* Id of the Application
* Package information
* Data of Approval/Rejection
* Platform (iOS or Android)
* Trust Score of the Application

Following information is displayed for the Apps whose EULA is not reviewed:

* Name of the Application
* Id of the Application
* Platform (iOS or Android)
* Trust Score of the Application
* Link to EULA
* Action to Approve/Reject EULA

# Marketplace (TBD)

Not Implemented at the time of writing of this document.

Glossary

|  |  |  |
| --- | --- | --- |
| # | **Term** | **Description** |
|  | App Trust Score | App Trust Score is score between 0 & 100 indicating trust worthiness of the App.  Trust Score is computed by Appthority and is based on number of vulnerabilities in a mobile App. |
|  | EULA | End User License Agreement |
|  |  |  |
|  |  |  |