



Kony Management Console User Guide

Release V8 SP2

Document Relevance and Accuracy

This document is considered relevant to the Release stated on this title page and the document version stated on the Revision History page. Remember to always view and download the latest document version relevant to the software release you are using.

Copyright © 2018 Kony, Inc.

All rights reserved.

April, 2018

This document contains information proprietary to Kony, Inc., is bound by the Kony license agreements, and may not be used except in the context of understanding the use and methods of Kony, Inc., software without prior, express, written permission. Kony, Empowering Everywhere, Kony Fabric, Kony Nitro, and Kony Visualizer are trademarks of Kony, Inc. MobileFabric is a registered trademark of Kony, Inc. Microsoft, the Microsoft logo, Internet Explorer, Windows, and Windows Vista are registered trademarks of Microsoft Corporation. Apple, the Apple logo, iTunes, iPhone, iPad, OS X, Objective-C, Safari, Apple Pay, Apple Watch, and Xcode are trademarks or registered trademarks of Apple, Inc. Google, the Google logo, Android, and the Android logo are registered trademarks of Google, Inc. Chrome is a trademark of Google, Inc. BlackBerry, PlayBook, Research in Motion, and RIM are registered trademarks of BlackBerry. SAP® and SAP® Business Suite® are registered trademarks of SAP SE in Germany and in several other countries. All other terms, trademarks, or service marks mentioned in this document have been capitalized and are to be considered the property of their respective owners.

Revision History

| Date | Document Version | Description of Release |
|------------|------------------|---|
| 04/23/2018 | 3.0 | Document published for V8 SP2 GA |
| 12/29/2017 | 2.0 | <p>Document published for V8 SP1 GA</p> <ul style="list-style-type: none">• Added a note under the Creating a New Enterprise App > Step 1 : App Basics section• Added Error Messages• A note is added under Login > Authentication Scenarios• Added a note under Dashboard > Reports > Enterprise App Network Usage Report• Added a note under Prerequisites and Setup > Application Settings > How to Configure Captcha Settings section• Updated Deleting Active Directory section |

| Date | Document Version | Description of Release |
|------------|------------------|---|
| 10/09/2017 | 1.0 | <p>Document published for V8 GA</p> <ul style="list-style-type: none">• Renaming Enterprise Store Android Binary<ul style="list-style-type: none">• Enterprise Store• Device Enrollment• Active Directory and Kony Fabric Identity Users Unlock.<ul style="list-style-type: none">• Application Settings > Usage Settings• Users page• App Ratings and App Downloads Report• Enterprise Wipe Enhancements• Search/Filter apps with categories<ul style="list-style-type: none">• Enterprise Apps• Self-service Console Apps• Default Groups• Default Device Sets• Default Policies |

Table of Contents

| | |
|--|-----------|
| 1. Introduction | 9 |
| 1.1 Preface | 10 |
| 2. Authentication Scenarios | 13 |
| 2.1 Scenario 1 | 14 |
| 2.2 Scenario 2 | 17 |
| 2.3 Scenario 3 | 20 |
| 2.4 Scenario 4 | 23 |
| 3. On-premises - Login | 27 |
| 3.1 Management Cloud - Login | 28 |
| 4. How to Configure Custom Authentication | 29 |
| 5. Configuring Post Login Processor | 31 |
| 6. Prerequisites | 35 |
| 6.1 Authentication Settings | 36 |
| 6.2 Device Settings | 56 |
| 6.3 Application Settings | 77 |
| 6.4 Admin Email Settings | 120 |
| 6.5 Content Settings | 123 |
| 6.6 Custom Attribute Sets | 129 |
| 6.7 Branding | 137 |
| 6.8 Geo and Time Fence List | 153 |

| | |
|--|------------|
| 6.9 Language Settings | 165 |
| 6.10 Internationalization on Devices | 169 |
| 6.11 Working with Internationalization | 169 |
| 6.12 Event Log | 177 |
| 6.13 System Status | 181 |
| 7. Access Management | 187 |
| 7.1 Managing Access | 187 |
| 7.2 Users | 188 |
| 7.3 Groups | 207 |
| 7.4 Permission Set | 224 |
| 8. Device Registration | 256 |
| 8.1 Device Registration- Post Confirmation Details (Admin) | 257 |
| 8.2 Device Initiated Registration | 259 |
| 8.3 Enterprise Store | 277 |
| 9. Device Management | 309 |
| 9.1 Managing Devices | 309 |
| 9.2 Devices | 310 |
| 9.3 Device Details | 313 |
| 10. App Management | 350 |
| 10.1 App Classification | 351 |
| 10.2 Managing Apps | 351 |

| | |
|--|------------|
| 10.3 Policies | 352 |
| 10.4 Categories | 365 |
| 10.5 Enterprise Stores | 368 |
| 10.6 Enterprise Apps | 375 |
| 11. Content Management | 416 |
| 11.1 Files Overview | 418 |
| 11.2 Files User Interface | 418 |
| 11.3 Applying Actions to Files | 421 |
| 11.4 Folders Overview | 428 |
| 11.5 Folders User Interface | 428 |
| 11.6 Applying Actions to Folders | 439 |
| 11.7 Content Policies | 452 |
| 11.8 Applying Content Policies | 454 |
| 11.9 Content Repositories | 458 |
| 12. Self Service Console | 463 |
| 12.1 Login | 464 |
| 12.2 Home | 465 |
| 12.3 Devices | 470 |
| 12.4 Content Management - Self-Service Console | 473 |
| 12.5 Folders | 473 |
| 12.6 Applying Features of the Self-Service Console | 482 |

| | |
|--|------------|
| 12.7 File Details Page | 488 |
| 12.8 Applying Actions to Files | 489 |
| 13. Dashboard | 494 |
| 13.1 Viewing the Enrollment Summary Chart | 496 |
| 13.2 Reports | 499 |
| 14. Management Error and Information Messages | 532 |
| 14.1 Policy Messages | 532 |
| 14.2 Push Messages | 538 |
| 14.3 Store Messages | 545 |
| 15. Frequently Asked Questions | 562 |
| 15.1 Sending a Message to All Devices | 562 |
| 15.2 Sending a Message to all iOS devices | 565 |
| 15.3 Sending a Message to all Android devices | 571 |
| 16. Annexure | 583 |
| 16.1 Internet Explorer 9 Compatibility Issues | 583 |

1. Introduction

Kony Management Suite's Enterprise mobility management (EMM) - App Management Only software is a policy configuration and management tool for applications on smartphones and tablets.

The primary purpose of this software is to ensure that all applications and device users are in compliance with the IT Policies set by the company. This goal can be achieved in different ways.

To manage apps on any device, it must be registered. The management can choose to manage apps for only a few employee devices or all of them. The employee database can be imported from enterprise systems like Microsoft Active Directory. registered

Applications are added to the Enterprise Store through which they are distributed to appropriate users and groups. The Admin can choose to distribute apps with or without policies. Applications must be wrapped in order to be able to assign policies to them.

Application policies can also be applied to users and groups and therefore apply to the app on all devices registered with the users specified. Policies allow the administrator to control the usage of apps but not the content itself. For example, you can prevent cut, copy and paste for one particular application. Similarly, you can prevent application access during holidays.

All the EMM policies are dynamic and location specific. It is possible to set policies between different office locations, home and so on. Policies can also be applied within specified time ranges, thereby providing the administrators complete control over the life-cycle of an app.

1.1 Preface

Kony Enterprise Mobility Manager (EMM) is an all-encompassing approach to the secure use of company-owned and employee-owned mobile devices. EMM typically involves combination of Mobile Application Management (MAM), Mobile Content Management and Mobile Access Management.

EMM solution: Scenarios

- For employees who need to install and use the enterprise apps on their own devices.
- For an enterprise that intends to manage its applications through a web console.
- For applications that can be managed with policies based on the latest IT guidelines within the organization.

1.1.1 Purpose

This document helps you familiarize with Kony Enterprise Mobile Management and provide procedural information to use Management console, Self-service console, and enterprise store.

1.1.2 Intended Audience

The information in this guide is intended primarily for:

- **System Administrators:** Employees who implement and enforce the security structure, responsible for maintaining multi-user computer system, including a local area network (LAN), setting up user accounts, installing system-wide software, adding and configuring new workstations and so on.
- **Users:** Employees who use the EMM where the application is running and can access some or all of its features.

1.1.3 Formatting Conventions

The following formatting conventions are used throughout the document:

| Conventions | Explanation |
|---------------------|--|
| Monospace | <ul style="list-style-type: none">• User input text, system prompts and responses• File path• Commands• Program code• File names |
| <i>Italic</i> | <ul style="list-style-type: none">• Emphasis• Names of books and documents• New terminology |
| Bold | <ul style="list-style-type: none">• Windows• Menus• Buttons• Icons• Fields• Tabs• Folders |
| URL | Active link to a URL. |
| <i>Note</i> | Provides helpful hints or additional information. |
| <i>Important</i> | Highlights actions or information that might cause problems to systems or data. |

1.1.4 Supported Platforms

Supported Platforms are iOS, iPad, Android, Android Tablet, and Windows Phone 8.1. Other Device Operating Systems are not supported.

1.1.5 Contact Us

We welcome your feedback on our documentation. Write to us at techpubs@kony.com. For technical questions, suggestions, comments or to report problems on Kony's product line, contact support@kony.com.

2. Authentication Scenarios

There are four pages where users are required to authenticate themselves:

- Management Console
- Self Service Console Login
- Download Page (during the registration process)
- Enterprise Store login (device side)

Important: During the enrolment procedure, the device displays the pop-up dialog box, asking the permission to send notifications. If you do not enable the notification, the Enterprise Store loads repeatedly. To overcome this situation, you need to manually enable or disable the Notification under Settings > Notifications > Enterprise Store to receive notifications from the Enterprise Store if declined during enrolment.

Based on users' existence in multiple Active Directories (ADs) and sources, users need to provide domain and source details for authentication.

| Scenario | If | | | User need to provide authentication details as follows: |
|----------|------|------|-----------------|---|
| | AD 1 | AD 2 | Local Directory | |
| 1 | YES | NO | NO | Username and password: Authentication should directly happen. |
| 2 | YES | YES | NO | Username, password, domain: Because there are users from different domains, this resolution is necessary. Only after this is provided shall authentication take place. |

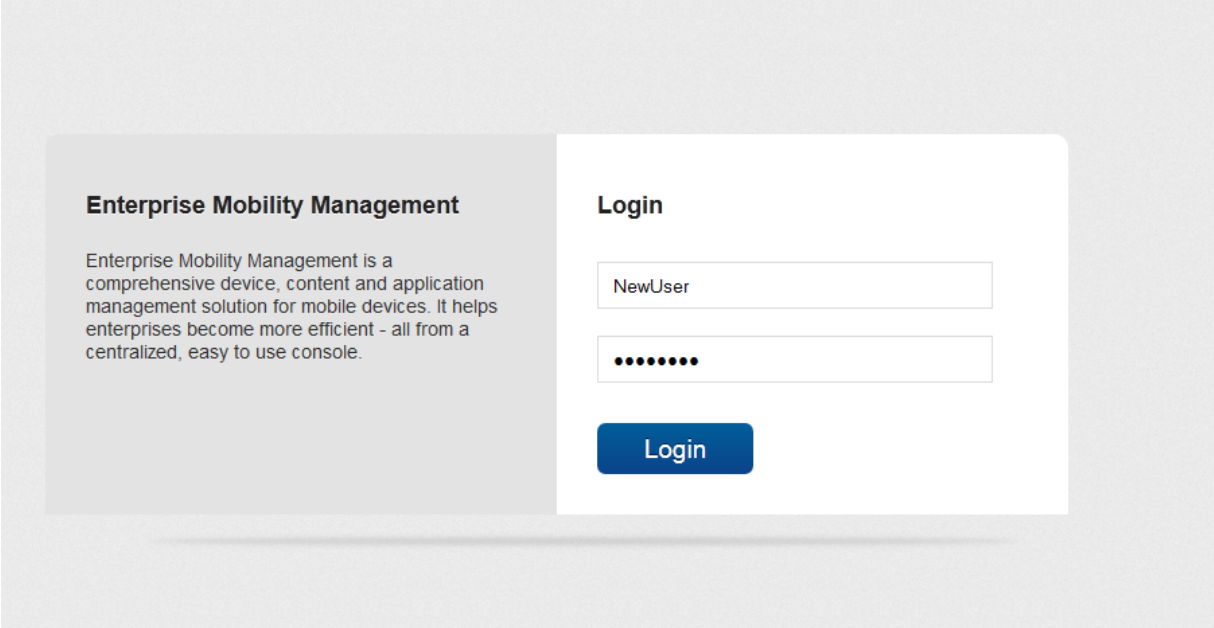
| Scenario | If | | | User need to provide authentication details as follows: |
|----------|------|------|-----------------|--|
| | AD 1 | AD 2 | Local Directory | |
| 3 | YES | YES | YES | Username, password, source, domain: Because there are users from multiple sources, both the Source and Domain should be differentiated. A user must provide both the Source and Domain before authentication occurs. |
| 4 | YES | NO | YES | Username, password, source: Because there are users from different sources but not domains, only the Source must be verified for authentication to occur. |

2.1 Scenario 1

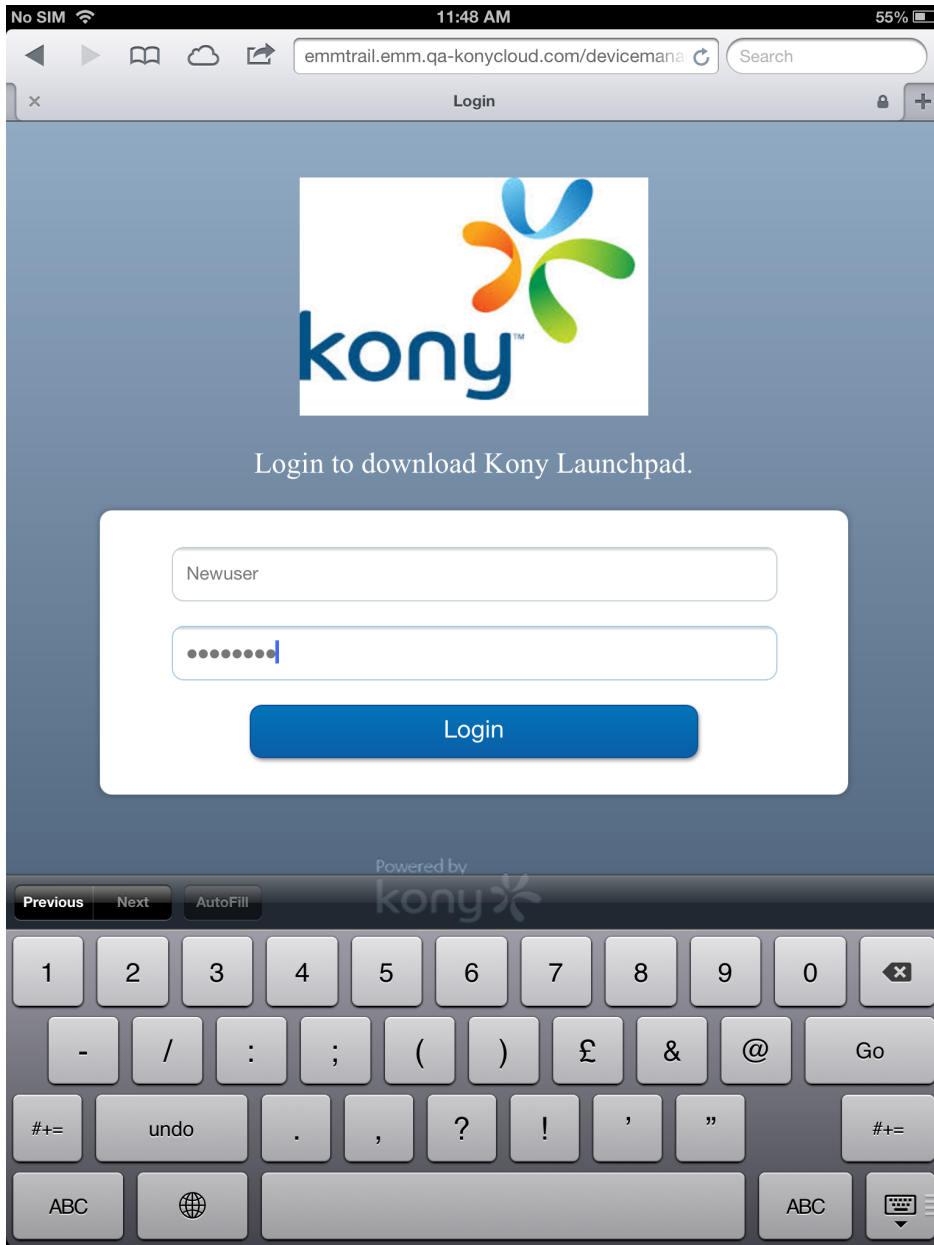
When a username is unique across domains and sources, a user is asked to provide a username and password. The system validates the user details and authenticates normally.

2.1.1 Management Console

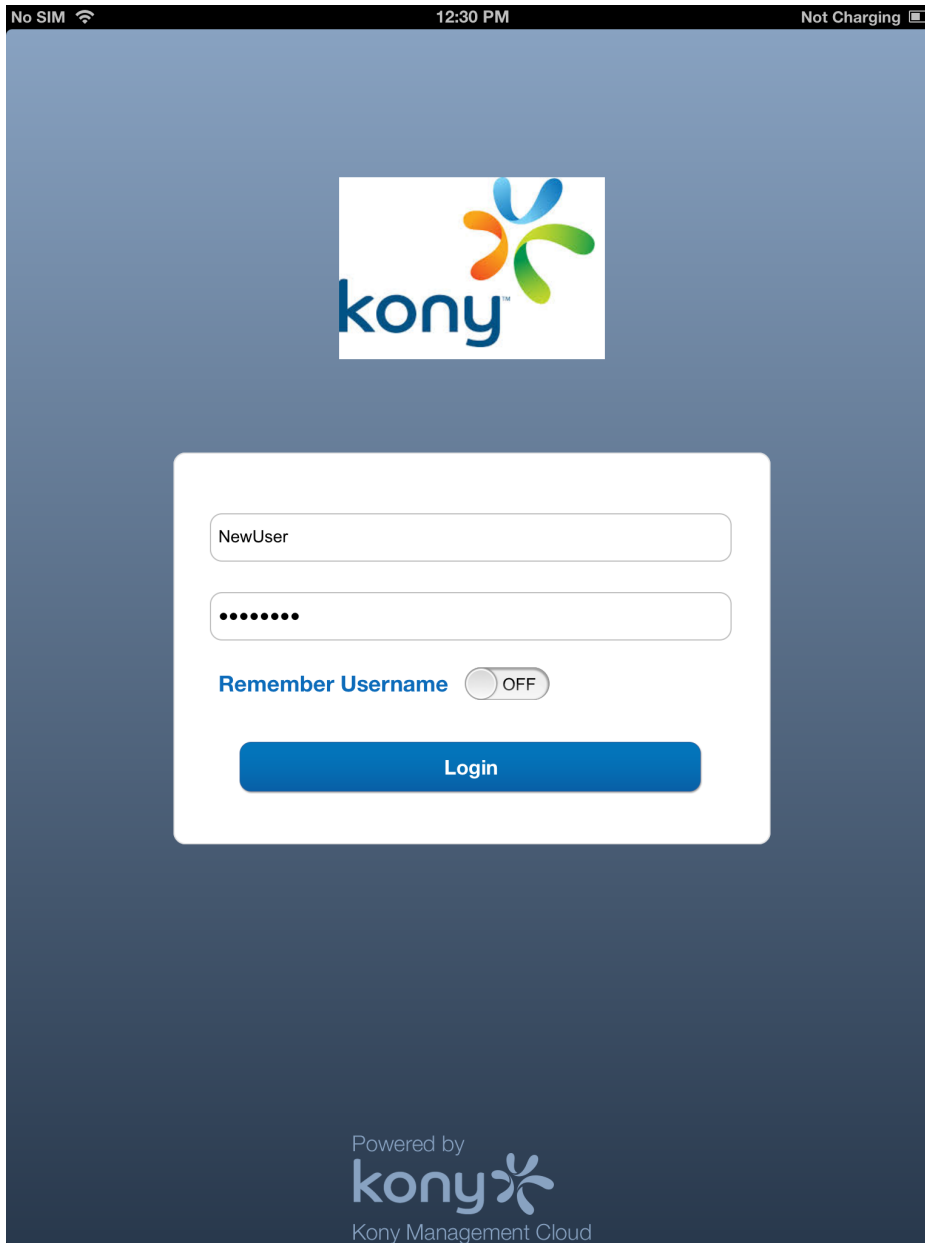
Self Service Console



2.1.2 Device download (device side)



2.1.3 Device log in (device side)



2.2 Scenario 2

When a username is common across domains and sources, a user is asked to provide the domain name that belongs to the user to complete authentication.

2.2.1 Self Service Console

Self Service Console

Enterprise Mobility Management

Enterprise Mobility Management is a comprehensive device, content and application management solution for mobile devices. It helps enterprises become more efficient - all from a centralized, easy to use console.

Login

hsireesha

.....

Select Directory

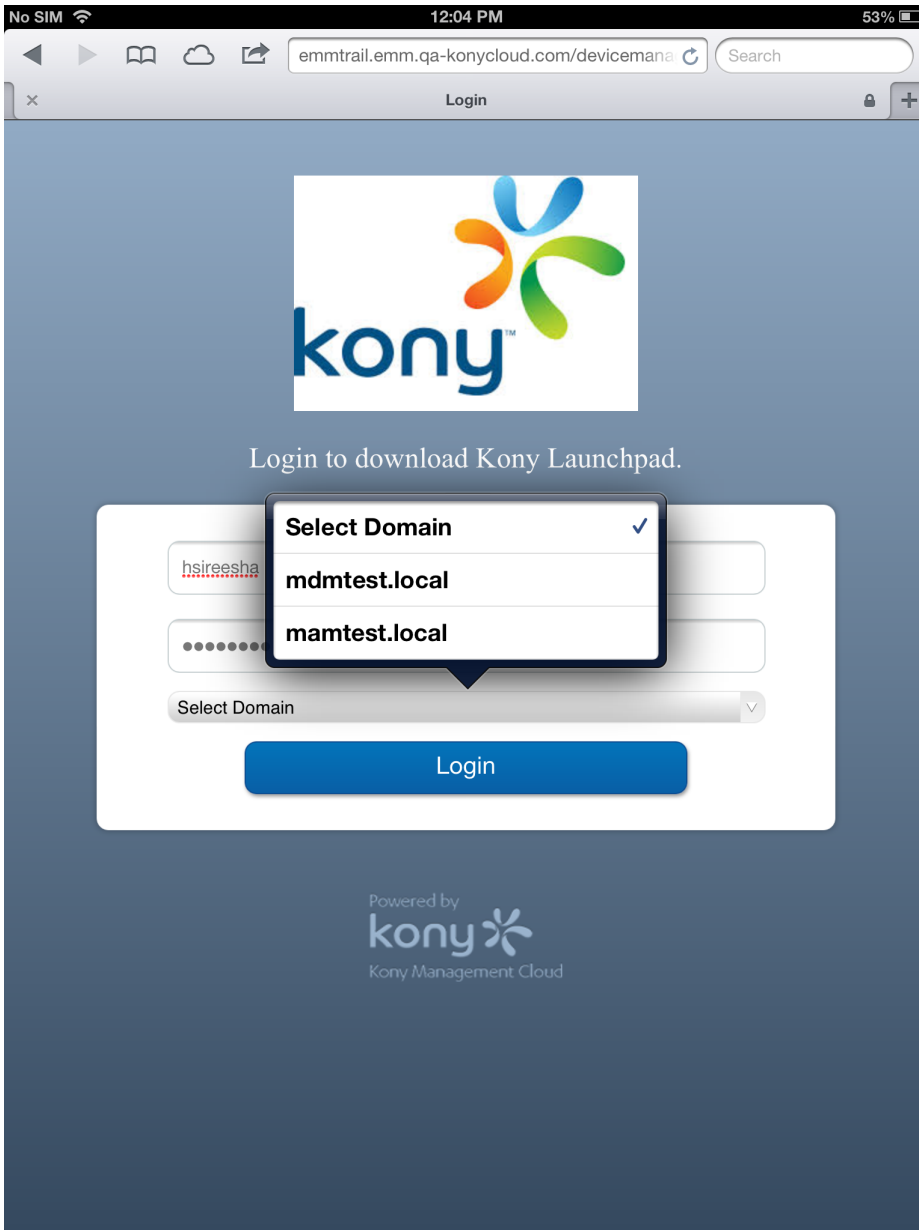
- Select Directory
- mdmtest.local
- mamtest.local

Login

A user can choose the remember me option - the browser saves the username, password and domain details. The next time the same page is accessed through the same browser, these details are already filled in. The user can modify any of the details.

If a user does not choose the remember me option, these fields will be blank the next time the page is loaded in the browser. Only the username and password fields will be displayed.

2.2.2 Device download (device side)



2.2.3 Device log in (device side)

The screenshot displays a mobile application interface for logging in. At the top, the status bar shows 'No SIM', signal strength, Wi-Fi, the time '12:08 PM', and battery level '52%'. The main content area features the Kony logo (a colorful flower-like icon above the word 'kony' in blue) centered on a dark blue background. Below the logo is a white login form with the following elements:

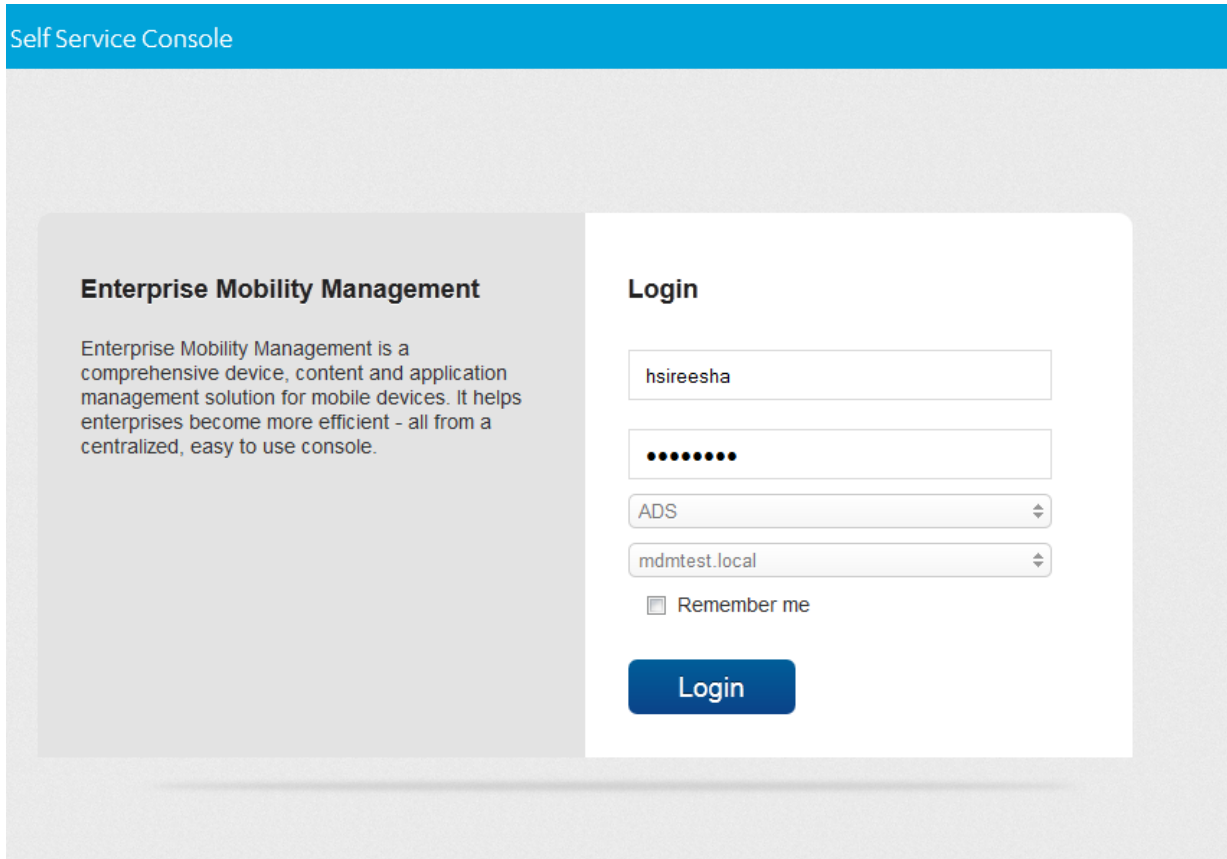
- A text input field containing the username 'hsireesha'.
- A password input field with masked characters represented by black dots.
- A dropdown menu showing 'mdmtest.local' as the selected domain.
- A 'Remember Username' toggle switch, currently turned 'ON'.
- A blue 'Login' button.

At the bottom of the screen, there is a dark navigation bar with three buttons: 'Previous', 'Next', and 'Done'. Below this bar is a list of domain options:

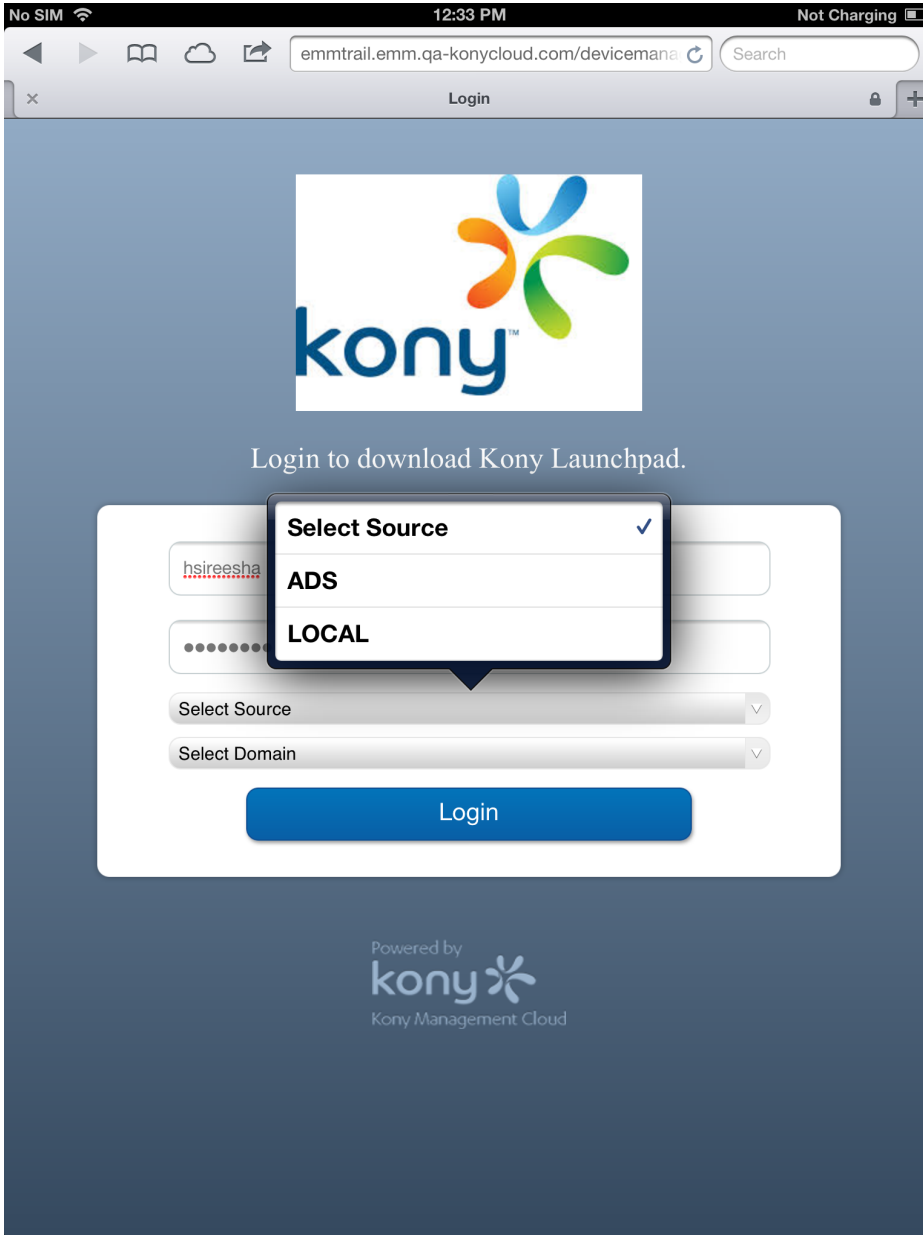
- mdmtest.local
- mamtest.local** (highlighted)

2.3 Scenario 3

When a username is common across multiple sources and multiple domains in Active Directory, a user is asked to provide source and domain details for authentication.



2.3.1 Device download (device side)



2.3.2 Device log in (device side)

The screenshot displays a mobile application interface for logging in. At the top, the status bar shows 'No SIM', signal strength, '12:37 PM', and 'Not Charging'. The main content area features the Kony logo at the top center. Below the logo is a white login form with the following elements:

- A text input field containing the username 'hsireesha'.
- A password input field with masked characters '.....'.
- A dropdown menu currently showing 'ADS'.
- A dropdown menu currently showing 'mdmtest.local'.
- A 'Remember Username' toggle switch, which is currently turned 'ON'.
- A blue 'Login' button.

At the bottom of the screen, there is a footer that reads 'Powered by kony Kony Management Cloud'.

2.4 Scenario 4

When a user is common across multiple sources but not across Active Directory, a user is asked to provide source details.

Self Service Console

Enterprise Mobility Management

Enterprise Mobility Management is a comprehensive device, content and application management solution for mobile devices. It helps enterprises become more efficient - all from a centralized, easy to use console.

Login

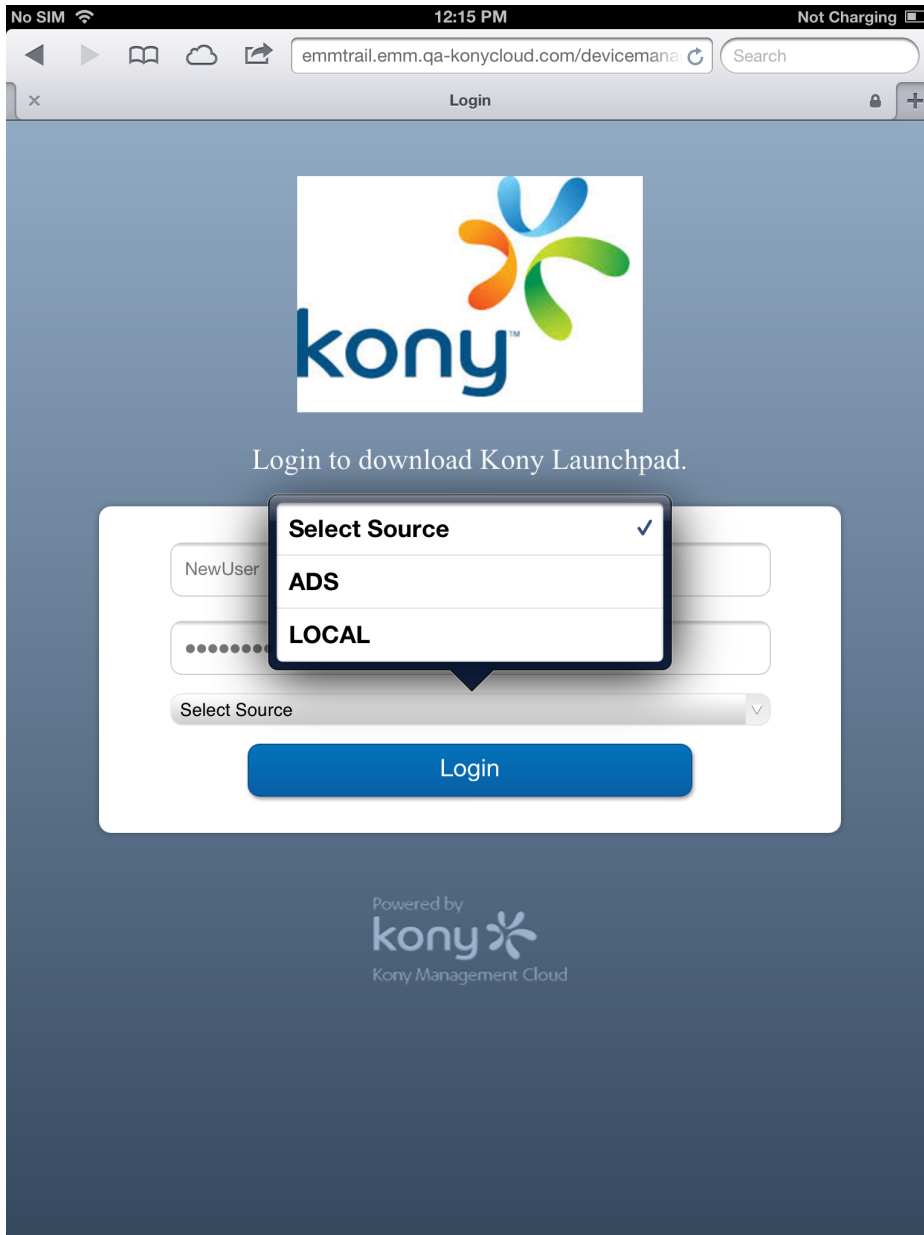
NewUser

.....|

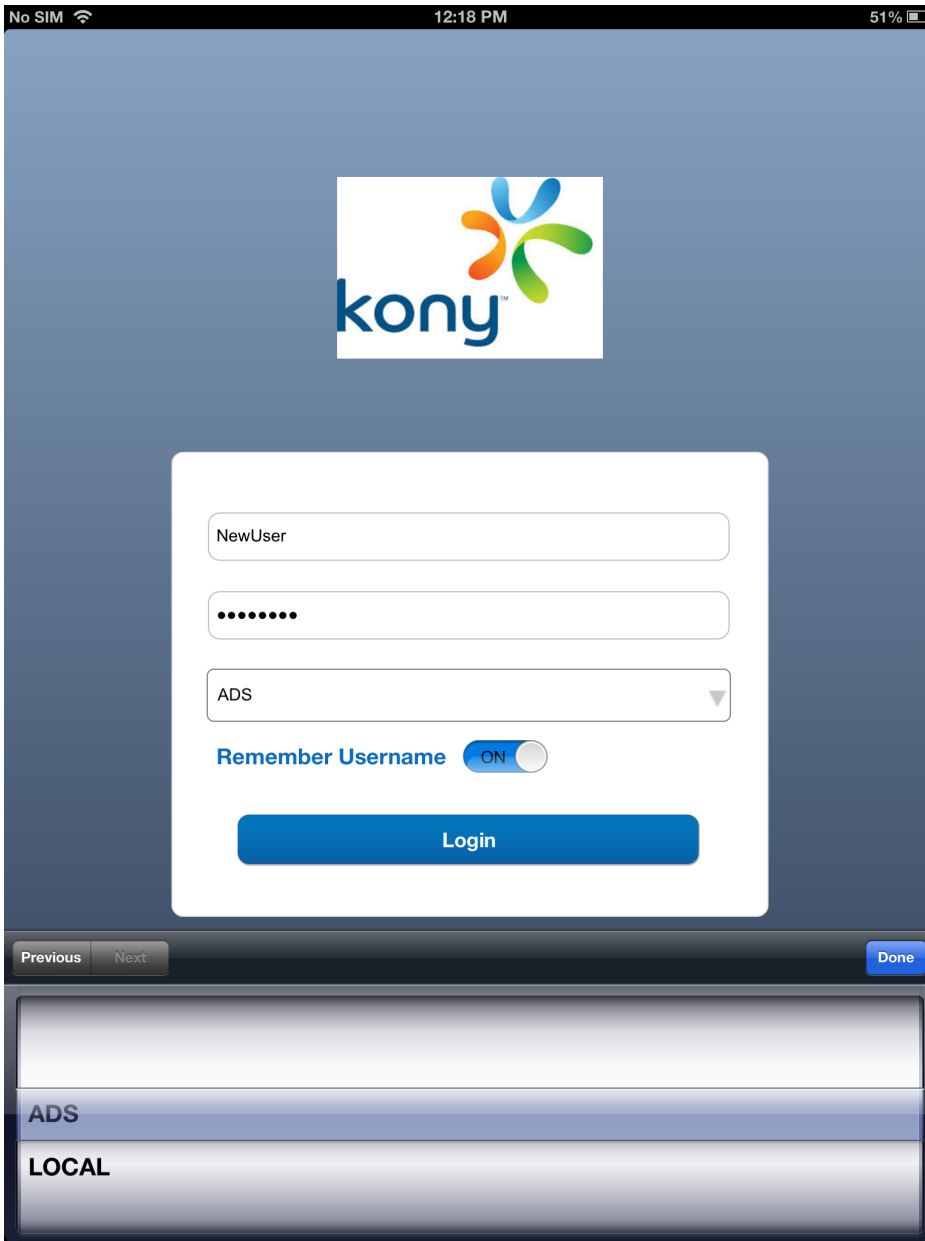
Select Source

- Select Source
- ADS
- LOCAL

2.4.1 Device download (device side)



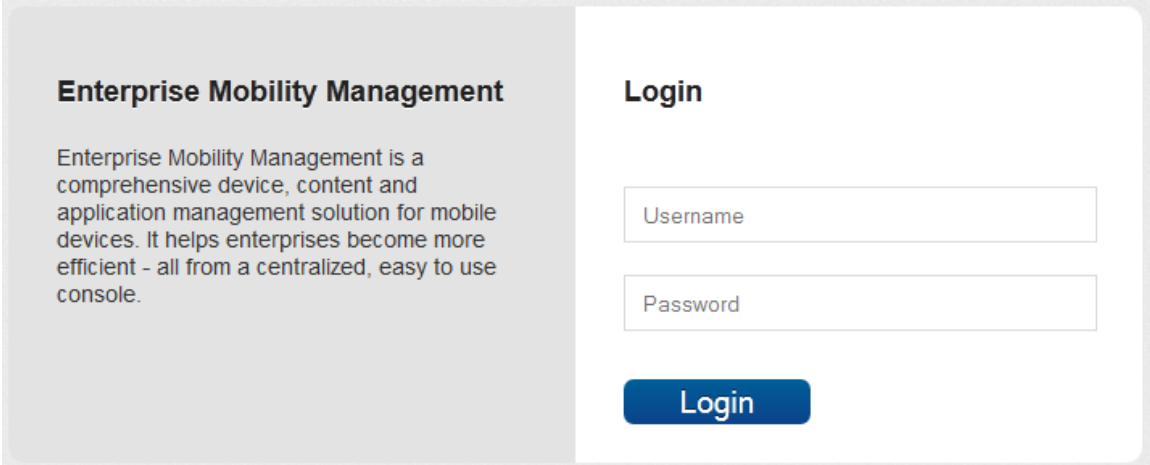
2.4.2 Device log in (device side)



3. On-premises - Login

The Kony EMM Console authentication window allows its users to log in to the system. The users with appropriate privileges can log in to EMM Console and perform various operations.

To log in to EMM Console, perform the following steps:



Enterprise Mobility Management

Enterprise Mobility Management is a comprehensive device, content and application management solution for mobile devices. It helps enterprises become more efficient - all from a centralized, easy to use console.

Login

Username

Password

Login

1. Open an Internet browser.
2. Enter the EMM URL in the Address field of the browser. The EMM Console Login screen appears.
3. **User Name:** Enter the user name in the User name text field.
4. **Password:** Enter the password in the Password text field.
5. Click the **Login** button. After successful authentication, Dashboard screen appears.

If the same user is logged into both the Admin and the Self Service Consoles and the user logs out from any of the Consoles, this results in closing both the active sessions. It may require the User to login into either Console again if they wish to access it.

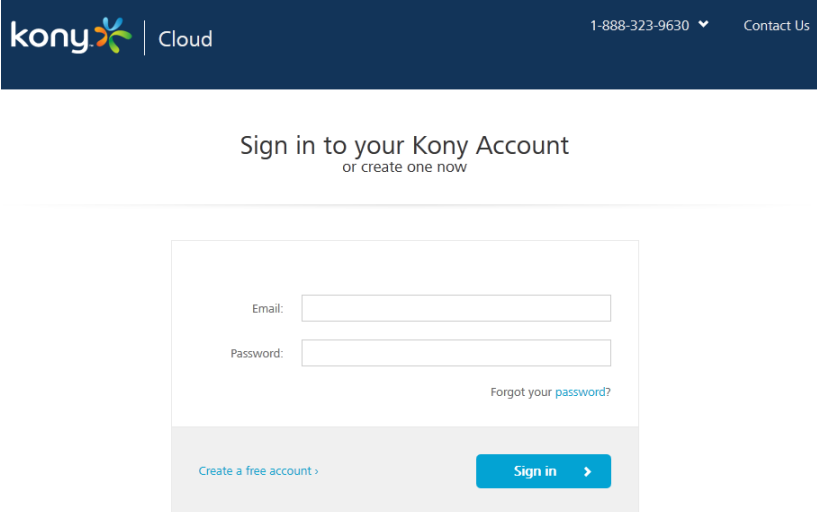
Note: It is recommended that the same User should not log in from multiple browsers or computers. Modifying the same page simultaneously may result into an unexpected behavior.

3.1 Management Cloud - Login

The Admin must log in to set up the EMM for the organization. The admin receives credentials from Kony for the trial version and/or post EMM license procurement. If you have not received Admin credentials, contact the sales representative or Support Team from Kony.

The application URL is provided by the Kony Team post EMM license procurement.

To log in to Management Cloud, perform the following steps:



1. Open an Internet browser.
2. Enter the EMM URL in the Address field of the browser. The EMM Console Login screen appears.
3. **User Name:** Enter the user name in the User name text field.
4. **Password:** Enter the password in the Password text field.
5. Click the **Login** button. After successful authentication, Dashboard screen appears.

4. How to Configure Custom Authentication

EMM provides a mechanism to build a custom authentication source. Custom Authentication feature provides additional flexibility to you to have all authentication happen against a source other than the directory configured. This authentication mechanism will be used for all authentication situations. When you configure custom authentication, the authentication source is modified but user interface and user experience will not be modified.

Important: You should be an expert at Java to perform the following steps. Do not follow these steps if you are not looking to implement custom authentication. Using the steps below without correct knowledge might result in abnormal behavior of the EMM console login.

This feature is available for on premises installation.

EMM provides a mechanism to configure a custom authentication mechanism or source. This enables clients to create

To configure custom authentication,

1. Create a java project with **CustomAuthProvider.java** class in it.
2. Implement **WebServiceAuthProvider** interface (located at **KonyUserMgmt-<version>.jar**) in the **CustomAuthProvider.java** file. You can provide multiple custom authentication provider classes.

Note: Custom provider class can also extend the **AbstractWebServiceAuthenticationProvider** (located at **KonyUserMgmt-<version>.jar**) abstract class and implement required methods. To implement custom authentication provider, you can refer the **AbstractWebServiceAuthenticationProvider** class.

3. Create a jar file from the java project.

4. Export the jar file to <EMM_WAR_HOME>/WEB-INF/lib/
5. Navigate to <EMM_WAR_HOME>/WEB-INF/classes/
6. Open the **config.properties** and enter your CustomAuthProvider fully qualified class names in the following format. For example,

- `authprovider.1=com.company.providers.CustomAuthProvider1`
- `authprovider.2=com.company.providers.CustomAuthProvider2`
- `authprovider.3=com.company.providers.CustomAuthProvider3`

7. Add any custom properties as required to the config.properties.

Note: You can access these values in custom implementation class using the `UserMgmtConfiguration.getVal(String key)` method. Implementation class will take care of handling exceptions and resource clean up.

5. Configuring Post Login Processor

When you authenticate by logging in, if you want certain activities to happen automatically, you can use the Post Login Processor feature. Post Login Processor feature enables you to build automated activities you want post login.

Important: You should be an expert at Java to perform the following steps. Do not follow these steps if you are not looking to configure post login processor. Using the steps below without correct knowledge might result in abnormal behavior of the EMM console login.

This feature is available for on premises installation.

To configure Post Login Processor,

1. Create a java project with **PostLoginProcessor.java** class in it. For example,

```
public interface PostLoginProcessor {  
    public void postAuthenticate(User user);  
}
```

2. Implement the **PostLoginProcessor** interface in the **CustomGroupSyncHandler.java** file. For example,

Note: After login, if you want to perform any specific tasks, for example, syncing user groups from external source, you can implement PostLoginProcessor.

```
package com.company;  
public class CustomGroupSyncHandler implements PostLoginProcessor  
{  
    private static final Logger LOG = LoggerFactory.getLogger  
        (CustomGroupSyncHandler.class);  
    private UserService userService = UsermgmtManagedBeans.getInstance
```

```
().getUserService());
private GroupService groupService =
UsermgmtManagedBeans.getInstance().getGroupService();
public void postAuthenticate(WebServiceAuthConfig config, User
user) throws WebServiceAuthException {
// Get proxy-aware HTTP client
Client client = config.getHTTPClient();
// or, get non-proxy aware HTTP client
// Client client = config.getNonProxyAwareRestClient();
/ Do a form post to the groups URL
WebResource usersresource = client.resource
(UserMgmtConfiguration.getVal("groupSyncUrl"));
Builder builder = usersresource.getRequestBuilder();
MultivaluedMap<String, String> formData = new MultivaluedMapImpl
();
formData.add("userName", user.getUserId());
ClientResponse response = builder.type(MediaType.APPLICATION_FORM_
URLENCODED_TYPE).post(ClientResponse.class, formData);
// Get group names from response - parse the response content and
get the groups.
// for example, if response will contain comma separated group
names for this user, split the response by comma (,)String groups
= response.getEntity(String.class);
Set<Group> userGroups = new HashSet<Group>();
Group group = null;
for(String groupId : groups.split(",")) {
// use GroupService.findGroupBySourceAndDomain(String groupId,
String source, String domain) to check if this group is already
present in EMM or not
group = groupService.findGroupBySourceAndDomain(groupId, "LOCAL",
user.getDomain()); // source can be one of UserSource enum types
(LOCAL, ADS, SAPHCM, OAUTH)
```

```
if(group == null) {
// this group is not present in EMM - first, save this group
group = new Group(groupId);
group.setDomain(user.getDomain());
groupService.saveOrUpdate(group);
}
// add group to the groups list
userGroups.add(group);
}

// associate all these groups to the user
user.setGroups(userGroups);

// update the user
userService.saveOrUpdate(user);
}
}
```

Note: If you want to have the option to modify the users and groups data in your database, use the following services and APIs in methods in the **CustomGroupSyncHandler.java** class. For example,

```
UsermgmtManagedBeans.getInstance().getUserService()
and
UsermgmtManagedBeans.getInstance().getGroupService()
```

3. Create a jar file from the java project.
4. Export the jar file to **<EMM_WAR_HOME>/WEB-INF/lib/**
5. Navigate to **<EMM_WAR_HOME>/WEB-INF/classes/**
6. Open the **config.properties** and enter your PostLoginProcessor class in it. For example,

```
auth.login.processor.post=com.company.PostLoginProcessor
```

7. Add any custom properties as required to the config.properties file.

Note: You can access these values in custom implementation class using the `UserMgmtConfiguration.getVal(String key)` method.

6. Prerequisites

Before you start managing the EMM Console, you need to configure the following settings:

1. [Authentication Settings](#)
2. [Device Settings](#)
3. [Application Settings](#)
4. [Admin Email Settings](#)
5. [Branding](#)
6. [Geo and Time Fence List](#)
7. [Event Log](#)
8. [System Status](#)
9. [Language Settings](#)

6.1 Authentication Settings

Companies maintain a store of users and their details. EMM provides a mechanism to either create a store of users in EMM (locally) or import from Active Directories. This information helps EMM provide resources such as registering devices and targeting apps. Users are unique for each source or domain. Kony Management suite supports the following authentication types.

- [Local](#)
- [Active Directory](#)
- [Kony Fabric Identity](#)

6.1.1 Local Directory

The Local Directory is available by default within EMM. It is a directory of all users created on EMM only by using the Add User. Local users are stored in EMM database.


6.1.2 Active Directory (AD)

ADs are external sources of users. Active Directories are the only third party sources supported for EMM.

Important: As an administrator, you must have the appropriate permissions to configure multiple Active Directory instances.

Once you have logged into the Management Console, from the left pane, click the **Authentication Settings** under the **Settings**. The Authentication Settings page appears with a list of Directories configured within EMM. You can search ADs.

The Directory List view displays the following columns:

| Column | Description |
|--|---|
| Domain | Displays the list of AD domains. |
| Directory Type | Displays the directory type of the AD. |
| Host or IP Address | Displays the list of host names or IP addresses. |
| Port | Displays the port numbers of the Active Directory Servers. |
| Created By | Displays the name of the administrator who created the configured Active Directory Servers. |
| Created On | Displays the date and time details of when Active Directory Servers configured. |
| Information Icon  | <p>Displays the number of users and groups imported from the Active Directory when you click on the information icon.</p> <p>If no users or groups are imported from a Directory, the information icon turns into a check box.</p> <p>If you want to delete an Active Directory, you must select the desired check box and then click the Delete button.</p> |
| Delete button | Deletes the selected Active Directory from the database. The Delete button dims because it is not available until a check boxes is selected. |

You can navigate the list view through the **Previous** and the **Next** buttons.

Active directories help ensure that only authenticated users and computers can access the network. These upcoming sections will help you learn more about managing your network resources:

- [Configuring Active Directory](#)
- [Configuring an AD with a Secured VPN for Management Cloud](#)
- [Searching and Filtering Active Directory](#)

- [Viewing Number of Users/Groups Imported from AD](#)
- [Updating Active Directory](#)
- [Deleting Active Directory](#)

6.1.2.1 Configuring Active Directory Settings

The Authentication Settings page is used to configure communication between EMM database and an AD. The EMM Console uses database to fetch employee details, to provide user authentication, and to update and synchronize users.

Once you have logged into the Management Console, under **Settings** from the left pane, click **Authentication Settings**. The **Directory List** page appears. Click the **+New Directory** button. The Authentication Settings page appears with directory list. Click on any of the directory, the Directory Details page appears with two tabs: Configuration and Synchronization.

Directory Details

Directory Settings > mdmtest.local

Configuration
Synchronization

Connection Configuration

Directory Type Forest No Forest

Recommendation Do not add sub-domains of a forest as a separate directory. It may result in erratic behavior on EMM

Root Domain *

Root IP Address *

Port Number *

Login Attribute User logon name

Username*

Password*

Search Base

 Search Base will be used for test connection only.
 If unspecified, Search Base will default to root domain.

Require Secure Connection Yes No

Note The default port number for this configuration is 3268

Configuration Tab

There are two types of ADs can be configured:

- Forest
- No Forest

A Forest AD can have multiple sub-domains under the same. A No Forest AD on the other hand has only one domain associated with it.

To configure the ADs, follow these steps:

1. Select the **Directory Type**. By default this is set to **No Forest**. If you want to configure Forest AD, go to [Step 2](#) in the below procedure and continue, else skip to [Step 3](#) to continue with No Forest AD.

2. Click the **Forest** option if you want to configure for the Forest AD.

The system displays the **Root Domain** and the **Root IP Address** fields.

| | |
|------------------------|--|
| Directory Type | <input checked="" type="radio"/> Forest <input type="radio"/> No Forest |
| Recommendation | Do not add sub-domains of a forest as a separate directory. It may result in erratic behavior on EMM |
| Root Domain | <input type="text"/> |
| Root IP Address | <input type="text"/> |

Following are the three types of groups of Forest ADs:

- **Universal**: These Groups are universal across entire forest. When the Group type is universal, the system imports all user references into EMM while importing users from the group.
- **Global**: When the Group type is Global and if it belongs to a sub-domain, the system does not import the user references while importing users from it.
- **Domain Local**: If the Group type is Domain Local and if it belongs to a sub-domain, the system does not import the user references while importing users from it.

In case of Forest AD configuration, not all Groups can be imported (with User association in tact). Only Universal Groups can be imported from sub-domains. From root domain, all Groups can be imported.

3. Type the required domain details:

Important: Do not add sub-domains of a Forest as a separate directory. While synchronizing Users and Groups, if common Users and Groups are found, it may result in erratic behavior.

If directory type is **Forest AD**, follow these steps:

- a. **Root Domain:** Enter the Root Domain name of the Forest AD.
- b. **Root Host Name or IP Address:** Enter the Root Host Name or IP Address of the Forest AD.

Or

If directory type is **No Forest AD**, follow these steps:

- a. **Domain:** Enter the Domain name of the AD.
- b. **Host Name or IP Address:** Enter the Host Name or IP Address.

Note: If you are configuring AD for Management Cloud, you need to configure a secure VPN for Cloud. To configure an AD with a Secured VPN for Cloud, refer to [Secured VPN for Cloud](#).

4. Enter the required server connection details:

- a. **Port Number:** Enter the port number of the AD Server.

Refer to the Note at **Require Secure Connection** field for default and recommended ports. You may choose to provide your own ports.

- b. **Login Attribute:** Select one of the attributes from the **drop-down** list to search AD.
- c. **User Name:** Enter the user name that is used to access the EMM server.
- d. **Password:** Enter the password that is used to access the EMM server.

- e. **Search Base:** Enter the domain context.

A Domain Context is a client-side representation of a domain service, providing access to all the functionality of the service.

For **No Forest**, if no context is specified, the system searches all Users from the root of AD by default. If you want Users to be searched from a specific node of the AD, specify the context. All searches shall happen from this context only.

For **Forest**, the Context field is used for **Test Connection** only. It is a non-mandatory field. If unspecified, the default context is the root domain. All live searches (non-test connection) happen from the root domain only.

- f. **Require Secure Connection:** By default, this is configured to **No**. Click **Yes** if you wish to enable secure connection using LDAPS.

The port numbers are vary based on configuration. The system displays default and recommended port numbers as follows:

| Directory Type | If Secure LDAP = No | If Secure LDAP = Yes |
|----------------|---------------------|----------------------|
| No Forest | 389 | 636 |
| Forest | 3268 | 3269 |

- Click the **Test Connection** button. If the connection is established, a confirmation message appears.
- Click the **Save** button.

Save status message appears.

7. Click **OK** to return to the main page.

Important: In this application, wherever passwords need to be provided, some browsers may ask to Remember Password. Opt for Never as it is irrelevant. Your enterprise passwords should not be remembered

Synchronization Tab

Once communication with ADs are configured, admin can configure synchronization of ADs based on time, days or weekly basis to get the latest information of Users or any newly added Users.

Synchronization can be done in one two ways:

- **Sync Timings:** admin configures sync jobs.
- **Sync Details:** admin initiates this process manually.

Directory Settings

Directory List > Directory Settings

Configuration Synchronization

Sync Timings

Directory Sync Start Time

Directory Sync Period

Custom Period Hours Days Weeks

Sync Type Imported All

Sync Details

| | |
|---|--|
| Directory Sync Status | Synchronization in Progress |
| Directory Sync Status | Synchronization Completed <input type="button" value="Sync All"/> <input type="button" value="Sync Imported"/> |
| <small># - Dev Note: Only one of these 2 status shown, In case No Sync happen status ="</small> | |
| Last Directory Sync Start Time | 08 Oct, 2013 09:08:12 EST |
| Last Directory Sync Completed Time | 08 Oct, 2013 09:08:12 EST |
| Next Directory Sync Start Time | 08 Oct, 2013 09:08:12 EST |

To configure the synchronization, follow these steps:

1. **Synchronization Start Time:** Place cursor in **Synchronization Start Time** field.

The screenshot shows the 'Sync Timings' configuration interface. It includes a 'Synchronization Start Time' input field with a placeholder 'mm/dd/yyyy HH:mm'. A calendar for November 2013 is open, showing the 28th selected. Below the calendar, the time is set to 14:29, with sliders for Hour and Minute. Buttons for 'Save', 'Reset', and 'Delete' are visible at the bottom left of the window.

The Calendar appears.

2. Select the **Date** and **Time** (Hour: Minute) and click **Done**.

The selected Date and Time appears in the field.

The screenshot shows the 'Synchronization Period' drop-down menu. The menu is open, showing options: Daily, Hourly, Daily, Weekly, Monthly, and Others. The 'Hourly' option is currently selected.

3. **Synchronization Period:** Select the synchronization period from the drop-down list.
4. **Custom Period:** Select the one of the options to customize the sync job based on Hours, Days, or Weeks.

5. **Synchronization Type:** By default, this option is set to **Imported**. This option synchronizes users who are imported into the EMM database.
6. Click the **Save** button. In the success message that appears, click **OK** to return to the main page.

Note: If an already registered Local user is overwritten with an AD User, then Block Email functionality does not work.

Sync Details

1. Click one of the buttons for Directory Sync Status.

Directory Sync Status: If the sync job is in progress, the system displays the status as "*Synchronization in Progress*".

Note: If a sync job in progress, the Sync All and the Sync Imported buttons will be inactive.

- **Sync All:** Click this button to synchronize all Users from the Directory.
- **Sync Imported:** Click this button to synchronize only imported users from the Directory.

Last Directory Sync Start Time: Displays the last Directory sync when started.

Last Directory Sync Completed Time: Displays the last Directory sync when completed.

Next Directory Sync Start Time: Displays the next Directory sync when scheduled.

2. Click the **Save** button. In the success message that appears, click **OK** to return to the main page.

Filtering Active Directories

You can search desired AD through the available search filters. You can apply a single or a combination of search filters to define the search criteria and get the refined outcome.

The Admin can click on the one of the table headers. Based on the sorted element, the system sorts the entire directory list to either ascending or descending order. The system displays an indicator to show if the sort is in ascending or descending order.

If the sort is in ascending order, the sort order is Numeric [0-9], Alphabetic [a-z, A-Z], Special characters.

Admin can also manually sort on the basis of all columns.

Filtering

Admin can enter text in the text fields to filter the column. The text must be at the beginning of each word of the column entry.

The system will filter all elements of the column based on the search term present in the column.

For example, If Admin types "Herm" or "herm", and presses the **Enter** key, then the system displays all directory names that contain **herm**. For example, Herman Melville, Herman Schultz, Kermit Hermit and Sherman.

The following columns have textual filters:

- Domain
- Host or IP Address
- Port

Filtering from Drop-down list

An administrator can filter data by one of the following options:

- Created By
- Created On

| Filter | Description |
|---|--|
| <p>Created By:</p> <ul style="list-style-type: none"> ■ Admin 1 ■ Admin 2 ■ Admin 3 | <p>The server only displays those directories (rows) that have the filtered entity.</p> <ul style="list-style-type: none"> • For example, if the directory name is Orlando AD, then all directories named Orlando AD are shown regardless of domains. <p>Filters can be applied for one or more columns. If filters are applied across multiple columns, the system performs AND condition between all filters.</p> <ul style="list-style-type: none"> • For example, if directory name is Orlando AD and Created By is Mike, then all directories created by Mike are shown. |
| <p>Created On:</p> <ul style="list-style-type: none"> ■ Today ■ Yesterday ■ Last 7 days ■ Last 10 days ■ Last 30 days ■ More than 30 days | <p>You can specify dates and time with the Created On filters. The filters represent data based on the following:</p> <ul style="list-style-type: none"> • Today - Displays list of ADs created on a system's current date. • Yesterday - Displays list of ADs created on yesterday's date. • Last 7 days - Displays list of ADs created between yesterday and 7 days ago. <p>For example, if today's date is June 20 and if you search for "Last 7 days", the system displays a list of ADs created between June 18 and June 12.</p> <p>All the above ranges are non-overlapping and ensures that no results are double counted.</p> |

6.1.2.2 Viewing Number of Users or Groups Imported From an Active Directory

From the Directory List page, you can view the details on how many users and groups are imported.

Note: When there are no users or groups imported from an Active Directory (AD), the information icon turns into a check box. To delete an AD, you select the desired check box and then click the Delete button.

To view the details, click the information icon next to Domain column. The system displays the details of users and groups imported from the AD.

You can click anywhere outside of the dialog to close it.

6.1.2.3 Updating Active Directory Settings

You may need to update an AD settings for specific reasons, for example, you may need to update a port number or its search base.

From the Directory List page, click one of the AD in the **Domain** column.

Directory List

+ New Directory

| <input type="checkbox"/> | Domain | Host or IP Address |
|---------------------------------------|---|---|
| | <input type="text" value="Search Domains"/> | <input type="text" value="Search Hostname/IP"/> |
| | mdmtest.local | mdmads.manage.kony.com |
| | mamtest.local | 10.11.12.76 |
| <input type="button" value="Delete"/> | | |

The Directory Settings page appears.

The desired fields can be updated. There are no restrictions. Once an AD is updated, it must be saved again to come into effect.

6.1.2.4 Deleting Active Directory

To delete an **Active Directory**, imported Users and Groups of the active directory should be deleted first. To delete all users and groups from an active directory, an admin can either use the bulk action feature from the **Users and Groups** pages or the admin can use the **Purge** button on the pop-up box after clicking the Information icon. Following either action, when no more users or groups from a particular AD have been imported into EMM, the Information icon changes into a checkbox and the AD can be deleted.

Note: When there are no Users and Groups imported from that AD, only then the Information icon turns into a check box.

To delete a Directory, follow these steps:

1. Select the check box for an AD entry next to the Domain.
2. Click the **Delete** button.

The system displays Delete Directory Confirmation Message: *"The chosen Directories shall be removed from the Directory list. Are you sure you want to do this?"*

3. Click **Yes** to confirm the deletion. The Directory is removed from the list.

6.1.3 SAP Directory

6.1.4 Kony Fabric Identity

Kony Management suite helps you to delegate Enterprise Store user authentication to Kony Fabric Identity service. Kony Fabric Identity service is part of Kony Fabric that validates users accounts and applications for authentication and authorization.

Kony Management suite allows administrators to configure Kony Fabric Identity service. Kony Management suite supports Kony Fabric Identity service as an alternative authentication mechanism only for the Kony Management Enterprise Store log-in.

Support is not provided for the following authentication scenarios.

- EMM Management Console
- EMM Self Service Console

Users authenticated through Kony Fabric Identity service are mapped to existing users in Kony Management. If a Kony Fabric Identity service user does not exist in Kony Management server, the user is created in Kony Management Suite. When you set the Kony Fabric Identity service authentication for the enterprise store, based on your Kony Fabric Identity service provider configured, you will be redirected to your Kony Fabric Identity service authentication page

The following are the identity providers supported by Kony Fabric Identity Service in Kony Management Suite:

- OAuth 2.0
- CA SiteMinder
- Microsoft Active Directory

Important: Kony Fabric Identity service is supported only for iOS and Android devices.

Directories

MobileFabric Identity

MobileFabric Identity Configuration

Use MobileFabric Identity Note : If activated, this will override all other authentication settings for EnterpriseStore login.

Identity Service Name * ?

Service Doc of MobileFabric App * ?

MobileFabric App Key * ?

MobileFabric App Secret * ?

Identity Service Url * ?

MobileFabric Token Validation ? Identity Server Public Key

Enable SSO ? Note : Wrapping and signing will trigger for iOS and Android Platforms if this setting is changed.

Enable Reverse Proxy Basic Auth ?

Kony Fabric Identity tab displays the following:

Kony Fabric Identity Configuration

- **Use Kony Fabric Identity:** When you select the feature, rest of the fields in the Kony Fabric Identity tab appear.
- **Identity Service Name:** Enter the Identity Service name that the Enterprise Store should use to authenticate the user. You can obtain the service name from the Publish screen by clicking the Key icon after the app is published to the server.

- **Kony Fabric App Key:** Enter the App key of the Kony Fabric back-end app that your Enterprise Store uses for authentication. You can obtain the app key from the Publish screen by clicking the Key icon after the app is published to the server.
- **Kony Fabric App Secret:** Enter the App secret of the Kony Fabric back-end app that your Enterprise Store uses for authentication. You can obtain the app secret from the Publish screen by clicking the Key icon after the app is published to the server.
- **Identity Service URL:** Enter the service URL of the Kony Fabric back-end app that your Enterprise Store uses for authentication. You can obtain this from the Publish screen by clicking the Key icon after the app is published to the server.
- **Service Doc of Kony Fabric App:** Enter the Service Doc details of the Kony Fabric back-end app that your Enterprise Store uses for authentication. You can obtain the service doc details from the Publish screen by clicking the Key icon after the app is published to the server.
- **Kony Fabric Token Validation:** Select the Kony Fabric token validation method, either with a preconfigured Kony Fabric Server or a public key.
 - **Public Key :** Enter the Public key details. The following two fields appear.
 - **Trust Auth URL:** Enter your Kony Fabric Tenants URL details.
 - **Trust Auth Cert:** Enter your Kony Fabric Tenants certificate details.
 - **Identity Server:** Select the option to validate your Kony Fabric Token using your Kony Fabric identity server details. Your Kony Management environment must already be configured in your Kony Fabric server. For more details, click [here](#).
- **Enable SSO:** Select the option to use single sign-on for apps built using Kony Fabric SDK.
 - **iOS Keychain Group:** Enter iOS keychain group details.
 - **Android Broadcast Passphrase:** Enter the passphrase for Android broadcast.

Note: For iOS, multiple SSO groups are not supported.

Note: If a child app exists before configuring Kony Fabric identity service settings, the child app must be re-wrapped.

Note: When a child app is re-wrapped, the entitlement.plist file is overwritten, and some features (for example, In app purchase) may not work.

Note: While using OAuth 2.0 for SSO, if you click on **Forgot Password** button and then return to the **Login** page to log in, you cannot log in to the Enterprise store. You need to kill the Enterprise store on your device and relaunch it.

- **Enable Reverse Proxy Basic Auth:** Selecting the option enables reverse proxy basic authorization. If your Kony Fabric Identity Server is behind a proxy server (for example CA SiteMinder), which needs basic authentication, select this option.
- **Save:** Click this to save the details you enter on the page.
- **Cancel:** Click this to cancel the changes you make on the page.

Note: If you change **AppKey**, **AppSecret**, and **Use SSO** settings, for iOS and Android platforms, wrapping will be triggered for Enterprise Stores.

6.1.4.1 How to Configure Kony Fabric Identity Settings

To configure Kony Fabric Identity settings, do the following:

1. In the Management Console, under **Settings**, click **Authentication Settings**. The Authentication Settings page appears.
2. Click the Kony Fabric Identity tab. The Kony Fabric Identity tab opens.
3. Select **Use Kony Fabric Identity**. More options appear.
4. In the **Identity Service Name** field, enter a service name.

5. In the **Service Doc of Kony Fabric App** field, enter the service doc details.
6. In the **Kony Fabric App Key** field, enter the app key.
7. In the **Kony Fabric App URL** field, enter the URL value.
8. From **Kony Fabric Token Validation**, select an option.
9. If you want to enable SSO, select **Enable SSO**.
10. In the **iOS Keychain Group**, enter the iOS keychain group name.
11. In the **Android Broadcast Passphrase** field, enter the passphrase for Android broadcast.
12. Select **Enable Reverse Proxy Basic Auth** to enable reverse proxy basic authorization.
13. Click **Save**. A confirmation message appears.
14. Click **OK**.

For more information on Kony Fabric Identity service, click [here](#).

For more information on Kony Fabric Identity App Key, App secret, and Service Doc, click [here](#).

6.2 Device Settings

The primary purpose of the Device Settings section is to configure the devices based on existing business rules. Once you log into EMM Console, from the left pane, click **Device Settings**. The **Device Settings** page appears.

Device Settings

Usage Configuration
Terms and Conditions
Message Templates
Communication Configuration

Set Time Zone Settings

Note Daylight Savings Time is automatically enabled but the UTC time difference may not be updated.

Display all Date Time in (UTC -5:00) Eastern Time (US & Canada), Bogota, Lima

Heartbeat Settings

Warning: Synchronization Time Period should not be less than the Sampling Frequency.

Sampling Frequency 4 Hours

Synchronization Time Period 8 Hours

Administrator Contact Settings

Warning: Without providing this, the Contact Support feature on User's devices shall not work.

Note To add multiple contacts provide Comma separated Email IDs (i.e. john@abc.com, tim@abc.com)

Support Email ID *

[Capture screenshot.](#)

Enrollment Settings

Allowed Enrollment Methods

Admin Initiated

Device Initiated Ownership Employee

Self Service Portal Initiated

Verify User Presence in AD Group Yes No

Enforce AD Group for Enrollment Configure

Enrollment Denied List View

Enterprise Store Settings

Timeout Period Custom 15 Minutes

Allow offline access on rooted devices Yes No Android

Mask Username on Enterprise Store Yes No

Watchdog Settings

Note #1 Devices continuously inactive beyond this limit will be purged

Note #2 Watchdog job is run once a day. If you modify the time limit below, changes will reflect in the next job cycle.

Device Inactivity Limit Never

Action Control Remove

Tracking Settings

Note #1 If Device Location Tracking setting is changed, then the Enterprise Store and Android Enterprise Apps will get re-wrapped and user will be required to upgrade the same on the device.

Note #2 Unless Enable Device Location Tracking is On, Geo-Fence policies will not work as expected.

Enable Device Location Tracking ? Yes No

Enable viewing device location ? Yes No

Allow Mock Location ? Yes No Android devices **Not supported from Android 6.0 onwards**

Allow User installed applications that have mock location permission ? Yes No Android devices

Enable Geo-fence based policies ? Yes No

SAFE Settings SAFE (Samsung Android 4.2+)

Enforce Android Safe(Samsung only) ? Yes No

Device Logs (Call/SMS/App/Network Usage)

Enable Device Logs ? Yes No

Enable AFW

Enable AFW ? Yes No

Mail+ for Enterprise

License Key

Save
Cancel

The screenshot shows the 'Usage Configuration' tab in the Kony Management Console. It contains three main sections:

- Set Time Zone Settings:** Includes a note about Daylight Savings Time and a dropdown menu for 'Display all Date Time in' set to '(UTC -5:00) Eastern Time (US & Canada), Bogota, Lima'.
- Administrator Contact Settings:** Includes a warning about Contact Support, a note about email IDs, and a text input field for 'Support Email ID'.
- Enterprise Store Settings:** Includes a dropdown menu for 'Timeout Period' set to '15 mins'.

At the bottom of the form are 'Save' and 'Cancel' buttons.

The device settings section enables you to configure devices based on existing rules in the Kony Management administrator console. The device settings section consists of the following tabs:

- **Usage Configuration:** In the usage configuration tab, you can configure various settings for the device for usage. You can do the following.
 - Set the default time that is applicable to all applications on the device
 - Configure the time in which data must transfer between the device and Kony Management administrator console.
 - Email of the administrator to contact for any issues
 - Configure enrollment settings where you can choose which enrollment modes are supported and which ones are restricted.
 - Settings for Enterprise store.
 - Tracking settings
 - SAFE settings

- Device Logs
- Mail Plus for Enterprise
- **Terms and Conditions:** Terms and Conditions are customizable agreements created by your organization outlining the conditions and policies that apply to the enrolled device and user. When an administrator updates existing Terms and Conditions, an email notification and push notification is sent to all active device users.

Device Settings page is used:

- To set [Usage Configuration](#)
- To set [Terms and Conditions](#)

6.2.1 Usage Configuration

The following table provides a list of UI elements in the Usage Configuration tab:

| Feature | Description |
|------------------------------|---|
| Set Time Zone Setting | Setting your timezone ensures that all date time elements in the entire application are shown as per your timezone. Use the drop-down list to select your timezone. |
| Heartbeat Settings | |
| Sampling Frequency | To set the time period for collecting and storing the device data in the EMM enterprise store, select the value from the drop-down list. |

| Feature | Description |
|---------------------------------------|---|
| Synchronization Time-Period | <p>To set the time period to sync between device and the EMM server, select the value from the drop-down list.</p> <p>Heartbeat configured in EMM applies only to iOS, Android, Windows 6.x, and Windows Phone 8 devices.</p> <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 10px; margin-top: 10px;"> <p>Note: If there is an insufficient memory on your device during transactions, enterprise store may stop communicating with EMM server. To resolve this issue, please ask users who faced this issue to restart the devices.</p> </div> |
| Administrator Contact Settings | |
| Support Email ID | <p>Enter the email id that you desire to configure as a support email. The email is included in the device app for users to contact. This field accepts any email-id. You are recommended to provide your support team's email ID.</p> |
| Enrollment Settings | |
| Allowed Methods | <p>Select the required check boxes to set device registration.</p> |
| Admin initiated | <p>If selected, the Admin can initiate the enrollment process. Single Device and Bulk Enrollment are allowed. Else they are not.</p> |
| Device Initiate | <p>If selected, the device can initiate itself without administrator intervention. Selecting the Device Initiated field will enable the following option:</p> <p>Ownership: Using the ownership field, you can globally flag all devices enrolling into EMM. Options are Corporate, Employee, and Shared.</p> |
| Self Service Portal | <p>If selected, the users can send requests to enroll their devices through the Self Service Portal.</p> |

| Feature | Description |
|--|---|
| Verify User Presence in AD Group | If Yes is selected, only users from ADs are allowed to enroll to EMM. By default, it is disabled. |
| Enforce AD Group for | If the Verify User Presence in AD Group option is Yes, only then the Configure button is enabled here. You can configure or add those users present in multiple AD Group, and only the selected Groups are allowed to enroll. |
| Enforcement Denied List | This contains a list of Devices that are not allowed to enroll and that are wiped from future enrollment. The administrator can modify this list accordingly. |
| Device Agent Settings | |
| Timeout Period | This sets the idle timeout for the device agent. Select the required timeout period from the drop-down list. If you choose Unlimited from the list, you will not be asked to authenticate on the enterprise store after initial sign in unless the password is changed. |
| Allow Log-in on Jailbroken/Rooted Devices | By default, this is set to No . Configure to Yes if you want to allow a jailbroken or rooted device from logging into the enterprise store. When a jailbroken or a rooted device tries to log into an enterprise store, the EMM server sends a notification with device details to the administrator |
| Allow offline access on rooted devices | This is available only when the Allow Login on Jailbroken/Rooted devices field is configured to Yes . Configure to Yes if you want to allow offline access on rooted devices. This is for Android devices. |
| Mask username on Enterprise Store | Configure to Yes if you want to mask the username on the enterprise store. Configuring this to yes will mask the user's username in the enterprise store login page and in the user profile. |
| Watchdog Settings | |

| Feature | Description |
|---|---|
| Device Inactivity Limit | You can set the limit for a number of days a device can be inactive. You can choose from the drop-down list available. |
| Action | You can choose an action to perform on the device. |
| Action Based On | Select one of the options from the list. Options include MDM Agent/enterprise store and Enterprise App. |
| Tracking Settings | |
| Enable Device Location Tracking | Using this feature, you can capture a device location in EMM. If set to Yes , the device location is captured. By default, this is set to No . |
| Enable viewing device location | Using this feature, you can view the location of a device. If this feature is set to No , you cannot view device location. Maps in EMM console and on the device will be hidden. |
| Enable Geo-fence based policies | Using this feature, you can enable the create a geofence feature for a device. If set to No , the Geofence page in the management console will be hidden. |
| Allow Mock Location | Using this feature, you can enable the create a geofence feature for a device. If set to No , the Geofence page in the management console will be hidden. |
| Allow User installed applications that have mock location permission | Using this feature, you can allow the user to install applications that use mock locations. |
| Communication Logs | |

| Feature | Description |
|---|---|
| Enable Device Communication Logs | Using this feature, you can enable EMM server to receive communication logs of a SAFE device. If configured to No , SMS and call logs cannot be collected from Samsung SAFE enabled devices |
| SAFE Settings | |
| Enforce Android SAFE (Samsung devices) | Using this feature, you can enforce the Android Safe feature on Samsung Android 4.2 and above devices. When configured to Yes , the Android Safe feature is enforced on applicable devices. When the feature is enforced, existing users are forced to log out. To continue using the enterprise store, users must log in again. |
| Device Logs (Call/SMS/App/Network Usage) | |
| Enable Device Logs | Using this feature, you can capture device logs for calls, SMS, app usage, and app network usage. Configure this to Yes to enable the fields below. |
| Enable Enterprise Application Usage | Configure this to Yes to capture an enterprise app's foreground usage details. Foreground app usage is the time an app is open on the device. |
| Enable Application Network Usage | Configure this to Yes to capture the network usage for an enterprise app. On Android devices, you can also capture the network usage details of public apps. |
| Enable Call Usage | Configure this to Yes to capture call logs on the device. |
| Capture all Phone Number | Configure this to Yes to capture phone number in the call log on a device. |
| Enable SMS Usage | Configure this to Yes to capture SMS logs on the device. |

| Feature | Description |
|---------------------------------------|---|
| Capture SMS Phone Number | Configure this to Yes to capture phone number in the SMS log on a device. |
| Capture SMS Text | Configure this to Yes to capture the SMS text on a device. |
| App Network Usage Capturing Frequency | <p>App Network Usage Capturing Frequency: Select a time period from the list. The server will capture network usage per app in the period selected. This is available only for Android devices.</p> <p>Note: The App Network Usage frequency must be less than that of the app submission frequency.</p> |
| Device Log Submission Frequency | Select a time period from the list. The enterprise store will submit device logs to the server in the interval selected. This is available for iOS and Android devices. |
| Enable AFW | |
| Enable AFW | By default, Android For Work is configured to No . If you want to use Android For Work for the Android devices, select Yes . This feature will not have any impact on the current configuration. This feature will impact the email device policy. Once the administrator saves the device settings, this will reflect on enrolled devices. |
| Mail + for Enterprise | |
| License Key | Enter the details of your Mail Plus license key. |

In the Usage Configuration tab, you can do the following:

- [Configure Time Zone for Devices](#)
- [Configure Device Heartbeat Settings](#)

- [Configure Administrator Contact Settings](#)
- [Configure Enrollment Settings](#)
- [Configure Enterprise Store Settings](#)
- [Configure Watchdog Settings](#)
- [Configure Tracking Settings](#)
- [Configure SAFE Settings](#)
- [Configure Device Logs](#)
- [Configure Mail Plus for Enterprise](#)

6.2.1.1 How to Configure Time Zone for a Device

To configure Time Zone settings, follow the steps below:

1. In Kony Management admin console, under **Settings**, click **Device Settings**. The Device Settings page opens with the Usage Configuration tab open by default.
2. Under the **Set Time Zone Settings** heading, from the **Display all Date Time in** list, select the time zone you want all the applications on the device to be in.
3. Click **Save**. A confirmation message appears.
4. Click **OK**. Your time zone settings are saved.

6.2.1.2 How to Configure Heartbeat Settings

In Kony Management suite, using the Heartbeat settings, you can synchronize data between an enrolled device and Kony Management suite at regular intervals. You can configure the heartbeat sampling frequency and the synchronization time-period.

To configure heartbeat settings, follow the steps below:

1. In Kony Management admin console, under **Settings**, click **Device Settings**. The Device Settings page opens with the Usage Configuration tab open by default.
2. Under **Heartbeat Settings** heading, from the **Sampling Frequency** list, select an option. For example, 5 minutes. The value configures the time period for collecting and storing the device data in the EMM enterprise store.
3. From the **Synchronization Time Period** list, select an option. For example, 1 hour. The value configures the time period to sync between device and the EMM server.
4. Click **Save**. A confirmation message appears.
5. Click **OK**. Your heartbeat settings are saved.

Heartbeat configured in EMM applies only to iOS, Android, Windows 6.x, and Windows Phone 8 devices.

Note: If there is insufficient memory on your device during transactions, enterprise store will stop communicating with EMM server. To resolve this issue, you must restart the affected device.

6.2.1.3 How to Configure Administrator Contact for a Device

Using this feature, you can configure an email as a support email ID to contact an administrator for any queries that a user may have. The email is included in the device app for users to contact. This field accepts any email ID. You are recommended to provide your support team's email ID.

To configure administrator contact settings, follow the steps below:

1. In Kony Management admin console, under **Settings**, click **Device Settings**. The Device Settings page opens with the Usage Configuration tab open by default.
2. Under **Administrator Contact** Settings heading, in the **Support Email ID** list, enter the email ID of the support that the user can reach to in case of any issues with the device. For example, support@yourcompany.com. This field accepts any email ID. Ensure that you provide the correct support team's email ID.

Important: If you do not provide this, the Contact Support feature on your device will not work.

Note: To add multiple contacts, provide commas to separate email IDs (i.e. john@abc.com, tim@abc.com).

3. Click **Save**. A confirmation message appears.
4. Click **OK**. Your administrator contact email ID is saved.

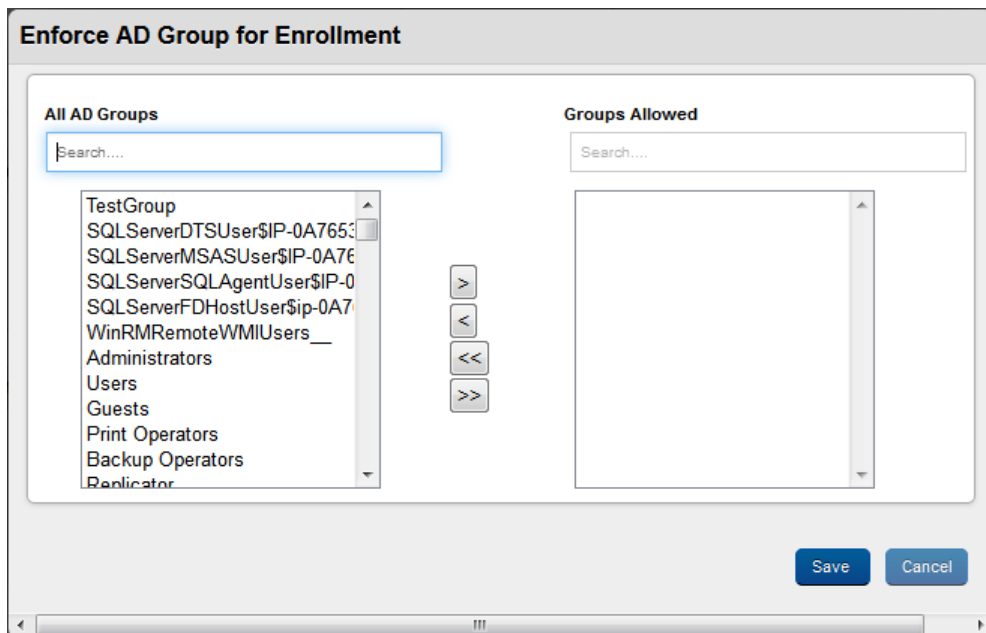
6.2.1.4 How to Configure Enrollment Settings

In this section, you can configure the enrollment settings as to which enrollment methods are allowed. You can also do additional tasks, such as verifying the presence of a user in an AD group, enforce a particular active directory group to enroll, and view the devices in the Enrollment Denied list.

To configure Enrollment settings, follow the steps below:

1. In Kony Management admin console, under **Settings**, click **Device Settings**. The Device Settings page opens with the **Usage Configuration** tab open by default.
2. Under the **Enrollment Settings** heading, configure the following:
 - i. To allow Admin initiated enrollment, select **Admin Initiated**.
 - ii. To allow device initiated enrollment, select **Device Initiated**. A new Ownership list appears. Using the ownership field, you can globally flag all devices enrolling into EMM. The options are **Corporate**, **Employee**, and **Shared**.
 - iii. From the drop-down list, select an option. For example, Corporate.
 - iv. To allow Self-service portal initiated, select **Self Service Portal Initiated**.
3. If you want to verify user presence in the Active Directory group, select **Yes**.

- To enforce active directory group for enrollment, click **Configure**. The Enforce AD Group for Enrollment window appears.
- From the **All AD Groups** column, move the group you want to allow enrollment to the **Groups Allowed** column.



Note: If you do not select any AD Group, then all users are allowed to enroll.

- Once you finish adding your groups, click **Save**. A success message appears.
- Click **OK**.
- Click **View** next to the Enrollment Denied list to view the devices that are denied enrollment. This contains a list of Devices that are not allowed to enroll and that are wiped from future enrollment. The administrator can modify this list accordingly.
- Click **Save**. A confirmation message appears.
- Click **OK**. Your Enrollment Settings are saved.

6.2.1.5 How to Configure Enterprise Store Settings

Using the Enterprise Store settings, you can configure the timeout period for the enterprise store and a few other settings related to installing enterprise store on rooted devices.

To configure Enterprise Store settings, follow the steps below:

1. In Kony Management admin console, under **Settings**, click **Device Settings**. The Device Settings page opens with the **Usage Configuration** tab open by default.
2. Under the **Enterprise Store Settings** heading, from the **Time Period** list, select **Custom**. A new field appears. Enter the number of minutes after which you want to log out the user for being inactive from the enterprise store.
3. For the **Allow Login on Rooted devices** option, select **Yes**. This will allow a user with a rooted device to install enterprise store on it. Configure to **No** if you want to prevent a jailbroken or rooted device from logging into the enterprise store.
When a jailbroken or a rooted device tries to log in to an enterprise store, the EMM server sends a notification with device details to the administrator.
4. To allow offline access on rooted devices, in **Allow offline access on rooted devices**, select **Yes**. This is available only when the **Allow Login on Rooted devices** field is configured to **Yes**. Configure to **Yes** if you want to allow offline access on rooted devices. This is available for Android devices only.
5. To mask the username on the enterprise store, in **Mask Username on Enterprise Store**, select **Yes**. Configuring this to **Yes** will mask the user's user name in the enterprise store login page and in the user profile
6. Click **Save**. A confirmation message appears.
7. Click **OK**. Your enterprise store settings are saved.

6.2.1.6 How to Configure Watchdog Settings

Watchdog is an electronic timer that is used to find any computer malfunctions and recover from it. In Kony Management suite, watchdog settings are used to configure a device's inactivity time, take action on those devices that do not comply with the set parameters.

To configure watchdog settings, follow the steps below:

1. In Kony Management admin console, under **Settings**, click **Device Settings**. The Device Settings page opens with the **Usage Configuration** tab open by default.
2. Under the **Watchdog Settings**, from the **Device Inactivity Limit** list, select **Custom**. A new field appears. Enter the device allowed inactivity in days.

Note: Devices continuously inactive beyond this limit are purged. Watchdog job is run once a day. If you modify the time limit, changes will reflect in the next job cycle.

3. From the **Action** list, you can choose an action to perform on the device.
4. From the **Action Based on** list, select one of the options from the list. Options include MDM Agent, enterprise store, and Enterprise App. If you select Enterprise App, the following fields are enabled:

Note: If you do not select Enterprise app usage under Device logs, you receive an error message. Enable Enterprise App Usage under Device Logs and then select Enterprise App.

- a. **Android:** Select the enterprise Android app based on which the watchdog settings will trigger and the device will be marked as control remove.
- b. **Android Tablet:** Select the enterprise Android tablet app based on which, the watchdog settings will trigger and the device will be marked as control remove.

- c. **iPhone:** Select the enterprise iPhone app based on which the watchdog settings will trigger and the device will be marked as control remove.
 - d. **iPad:** Select the enterprise iPad app based on which the watchdog settings will trigger and the device will be marked as control remove.
 - e. **Windows:** Select the enterprise Windows app based on which the watchdog settings for enterprise corporate data wipe will be activated.
5. Click **Save**. A confirmation message appears.
 6. Click **OK**. Your Watchdog settings are saved.

6.2.1.7 How to Configure Tracking Settings

In Kony Management suite, the tracking settings section helps you to know the location of a device, apply a geofence policy on a device, and to configure allowing mock location for apps.

To configure tracking settings, follow the steps below:

Note: When you modify Device Location Tracking settings, enterprise store will be re-wrapped. You must upgrade enterprise store on the device.

1. In Kony Management admin console, under **Settings**, click **Device Settings**. The Device Settings page opens with the Usage Configuration tab open by default.
2. Under the **Tracking Settings** heading, configure the following fields:
 - a. **Enable Device Location Tracking:** Using this feature, you can capture a device location in EMM. If set to **No**, the device location is not captured and the location feature in the enterprise store does not work.
 - b. **Enable viewing device location:** Using this feature, you can view the location of a device. If this feature is set to **No**, you cannot view device location. Maps in EMM console and on the device are hidden.

- c. **Enable Geo-fence based policies:** Using this feature, you can enable the create a geo-fence feature for a device. If set to **No**, the Geo-fence page in the management console are hidden.
 - d. **Allow Mock Location:** Using this feature you can allow applications to use mock location on a device.
 - e. **Allow User Installed applications that have mock location permission:** Using this feature, you can allow the user to install applications that use mock locations.
3. Click **Save**. A confirmation message appears.
 4. Click **OK**. Your tracking settings are saved.

6.2.1.8 How to Configure Communication Logs

In Kony Management suite, the communications logs feature helps you to keep a log of various communication made by a device.

To configure communication logs, follow the steps below:

Note: This feature is applicable for Samsung SAFE-enabled devices.

6.2.1.9 How to Configure SAFE Settings (for Android)

In Kony Management suite, using the Android native SAFE settings, you can configure the Samsung SAFE feature for Android devices.

To configure SAFE settings, follow the steps below:

1. In Kony Management admin console, under **Settings**, click **Device Settings**. The Device Settings page opens with the **Usage Configuration** tab open by default.

2. Under the **SAFE Settings** heading, select **Yes** for **Enforce Android Safe (Samsung only)**. This is applicable only for SAFE-enabled Samsung Android devices that are on Android version 4.2 onwards.
3. Click **Save**. A confirmation message appears.
4. Click **OK**. Your SAFE settings are saved.

Important: When the feature is enforced, existing users are forced to log out. To continue using the enterprise store, users must log in again.

6.2.1.10 How to Configure Device Logs

In Kony Management suite, the device logs feature helps you to keep a log of various activities on the device. The log information can include calls/SMS/app/network logs.

To configure Device logs, follow the steps below:

Important: Set all the fields to **Yes** to enable App Usage, Call Usage, SMS Usage, and App Network Usage reports.

1. In Kony Management admin console, under **Settings**, click **Device Settings**. The Device Settings page opens with the **Usage Configuration** tab open by default.
2. Under the **Device Logs (Call/SMS/App/Network Usage)** heading, select **Yes** for **Enable Device Logs**. More fields appear.
3. To create logs for enterprise application usage, select **Yes** for **Enable Enterprise Application Usage**.
4. To create logs for enterprise application network usage, select **Yes** for **Enable Application Network Usage**. Only android enterprise applications network usage can be captured using this field.

Note: The App Network Usage frequency must be less than that of the app submission frequency.

5. To create logs of call usage, click **Yes** for **Enable Call Usage**. This is applicable only for Android devices.
6. To capture the phone number of the device, select **Yes** for **Capture Call Phone Number**. This is applicable only for Android devices.
7. To capture SMS usage, click **Yes** for **Enable SMS Usage**. This is applicable only for Android devices.
8. To capture the number of the phone the SMS is sent to, select **Yes** for **Capture SMS Phone number**. This is applicable only for Android devices.
9. To know the contents of the SMS text, select **Yes** for **Capture SMS Text**. This is applicable only for Android devices.
10. You can configure the frequency at which the app network usage information is captured. From the **App Network Usage Capturing Frequency** list, select an option. For example, 4 hours. This is applicable only for Android devices.
11. You can configure the frequency at which the device logs are submitted to the Kony Management administrator console. From **Device Log Submission Frequency** list, select 6 hours. This is applicable for Android and iOS devices.
12. Click **Save**. A confirmation message appears.
13. Click **OK**. Your device logs settings are saved.

6.2.1.11 How to Configure Mail + for Enterprise

To configure Device logs, follow the steps below:

1. In Kony Management admin console, under **Settings**, click **Device Settings**. The Device Settings page opens with the **Usage Configuration** tab open by default.
2. Under the **Mail + for Enterprise Device** heading, in the **License key** text box, enter your license key for Mail + for enterprise.
3. Click **Save**. A confirmation message appears.
4. Click **OK**. Your Mail + settings are saved.

6.2.2 Terms and Conditions

Terms and Conditions are customizable agreements created by your organization outlining the conditions and policies that apply to the registered device and user. When an administrator updates existing Terms and Conditions, an email notification and push notification is sent to all active device users.

The screenshot shows the 'Employee Terms and Conditions' configuration window. At the top, there are four tabs: 'Usage Configuration', 'Terms and Conditions' (which is selected), 'Message Templates', and 'Communication Configuration'. The main content area is a rich text editor with a toolbar containing options for Format, Font, Size, Bold (B), Italic (I), Underline (U), Strikethrough (I~~x~~), Bulleted List, Numbered List, Indent, Outdent, Link, Unlink, and Image. The text area contains 't n c' and a 'body' label at the bottom right. Below the text area, there is a red warning message: 'Warning Please keep saving your work to avoid any data loss due to session timeout.' There are two checkboxes: 'Send Notification - Push' (checked) and 'Send Notification - Email' (unchecked). A note at the bottom states: 'Note Enrolled users will be notified with latest Terms and conditions in the above selected mode. If none of above notification mode is selected then user will not be notified with new changes.' At the bottom of the window, there are 'Save' and 'Cancel' buttons.

To define Terms and Conditions, follow these steps:

1. Enter terms and conditions in the Employee Terms text box. The text toolbar allows you to edit text.

2. To send a notification to the user, select one of the following options.
 - a. Send Notification - Push
 - b. Send Notification - Email
3. Click the **Save** button. In the confirmation message (Save Device Settings) that appears, click **Yes** to save changes. Another confirmation page appears.

Important: If you select **No**, the confirmation message closes and changes made are not saved.

4. Click **OK** to return to the terms and conditions page.

The following are various conditions for Push and email notifications:

- When an administrator makes changes to Terms and conditions, he can click on **Save**. A confirmation message appears. The administrator can choose to proceed to IF the When an administrator updates the Terms and Conditions on the server, a push notification is sent to all active users who have active devices.
- If the user is logged out of the enterprise store, Terms and Conditions appear to the user on next log in.
- A user can accept the terms and continue to use the Enterprise store. If a user denies new terms and conditions, Enterprise Wipe command will be sent to the device.
- An administrator can verify the reason for a device deactivation from Event logs.

6.3 Application Settings

The primary purpose of this section is to configure Application Settings to maintain several particulars, such as Enterprise Certificates, Provisioning Certificates, Usage Settings, Error Messages, Encryption Keys, VPP Apps, and Message Templates.

Application Settings

Certificates
Usage Settings
Error Messages
Encryption Key
VPP Apps
Message Templates

iOS

Note #1 : All certificates uploaded in this section following the distribution certificate have to be derived from the same.
Note #2 : Any .pfx certificates should be renamed to .p12 before uploading.

Enterprise Certificates

Note : The Bundle Identifier should be of type com (domain) *

Enterprise Distribution Certificate ⓘ

Certificate Pass Phrase

[Certificate Details](#)

Use wildcard provisioning profile?

Wild Card Provisioning Profile ⓘ

[Certificate Details](#)

Enterprise Store Certificates

Note #1 : The Bundle Identifier should be of type com (domain).containerapp, where (domain) matches with wildcard certificate
Note #2 : The Launchpad Push Certificate should be created before creating Launchpad provisioning profile
Note #3 : Ensure that the Apple Push Services (aps-environment) is enabled during Provision Profile creation.

Push Certificate ⓘ

Push Certificate Pass Phrase

[Certificate Details](#)

Enterprise Store Provisioning Profile ⓘ

[Certificate Details](#)

Android

GCM Key

Google ID

GCM key for Android ⓘ

Project number (Sender ID)

Key Store Credentials

Key Store ⓘ

Key Store Pass Phrase

Certificate Alias

Certificate Pass Phrase

[Certificate Details](#)

Google Maps API

Google Maps Android API V2 Key ⓘ

Note Kony will re-sign the Android Launchpad app based on the details provided here. Please click 'Certificate Details' and make sure that the SHA1 fingerprint and the launchpad package name (com.kony.mdmcilent) are appropriately associated with your Google account. In case any Android apps are submitted to EMM and they use Maps, then please make sure the SHA1 fingerprint and application package name are associated to that app's corresponding Google account. The SHA1 fingerprint is replaced as part of the app signing process, hence this task is necessary.

Windows

Enterprise Certificate

Certificate ⓘ [+ Add](#)

2-Way SSL

Note : Any certificate uploaded for 2-Way SSL will be renamed to twsc.p12

Certificate ⓘ [+ Add](#)

Save
Cancel

From the **Settings** section, click **Application Settings** from the left panel. By default, the **Certificates** tab is displayed. . The **Application Settings** Page includes five tabs:

- [Certificates](#)
- [Usage Settings](#)
- [Error Messages](#)
- [Encryption Key](#)
- [VPP Apps \(Volume Purchase Program for iOS 7+ devices\)](#)
- [Message Templates](#)

6.3.1 Certificates

The primary purpose to have certificates for iOS, Android, and Windows is to register and issue certificates to end users to configure mobile devices for certificate-based authentication.

In the certificates section, you can do the following:

- **For iOS:**
 - Upload app distribution certificate
 - Upload push notification certificate
 - Upload a wildcard provisioning certificate
 - Upload an enterprise provision certificate
- **For Android:**
 - Provide your GCM details to configure notifications from your server to your Android apps and from your Android apps to your server.
 - Provide details of your Keystore to ensure that your apps and your apps data are encrypted and secure.

- Link your Google Maps Android API key with your Google Maps-enabled Android enterprise apps.
- For Windows:
 - Link your Windows apps with your Windows Symantec ID to ensure data and app security.
- For Two-way SSL:
 - Link your apps with a two-way SSL certificate for mutual authentication in a secure manner.

Application Settings


Certificates Usage Settings Error Messages Encryption Key VPP Apps Message Templates

iOS

Note #1 : All certificates uploaded in this section following the distribution certificate have to be derived from the same.
Note #2 : Any .pfx certificates should be renamed to .p12 before uploading.


Enterprise Certificates

Note : The Bundle Identifier should be of type com.(domain).*

Enterprise Distribution Certificate 


Certificate Pass Phrase

Use wildcard provisioning profile?


Wild Card Provisioning Profile 

Enterprise Store Certificates

Note #1 : The Bundle Identifier should be of type com.(domain).containerapp, where (domain) matches with wildcard certificate
Note #2 : The Launchpad Push Certificate should be created before creating Launchpad provisioning profile
Note #3 : Ensure that the Apple Push Services (aps-environment) is enabled during Provision Profile creation.

Push Certificate 

Push Certificate Pass Phrase

Enterprise Store Provisioning Profile 

6.3.1.1 iOS

Apple uses various authentication mechanisms to ensure the security of iOS apps. Apps are distributed to devices in various ways (through the Appstore, privately distributed by enterprises and distributed by a company/developer internally with their teams for testing).

There are three important components in the authentication mechanism of Apple,

- **Distribution certificates:** Certificates authenticate you as an entity. They can represent you as a company or a developer.
- **Identifiers (device and app):** Identifiers are unique IDs. These unique identifiers exist for your iOS app as well as your Devices.
- **Provisioning profiles:** Provisioning profiles associate your certificates with your IDs and ensures that all these devices and apps are authentic.

Each of the certificates has a passphrase associated with them. You must provide the details of the certificate's passphrase when you upload any certificates to Kony Management. The certificate section for iOS allows you to add two certificates and two provisioning profiles.

Using the distribution certificate, you can distribute your apps across your team. Using the push notifications certificate, notifications will be sent to your apps from Kony Management administrator console. Kony Management uses your Apple distribution certificate to authenticate your apps.

The iOS section view displays the following elements:

| Feature | Description |
|-------------------------------------|--|
| Enterprise Distribution Certificate | Using this feature, you can add your Apple enterprise distribution certificate to the Kony Management server. To add the certificate, click +Add to select the certificate from its location and then click Open . The selected certificate with size in KB appears next to Enterprise Distribution Certificate label. |

| Feature | Description |
|---------------------------------------|---|
| Certificate Passphrase | Enter the password. While accessing, the certificate and the associated password must match. |
| Use wildcard provisioning profile? | Select this if you want to use the Wildcard provisioning profile. |
| Wildcard Provisioning Profile | <p>Using this feature, you can add your Apple wildcard provisioning profile to the Kony Management server. Click +Add to select the provisioning profile from its location and then click Open.</p> <p>Before uploading your app, you should have the distribution certificates for iOS. When the app is ready for publication, you can create the wildcard provisioning certificate.</p> |
| Push Certificate | Using this feature, you can add your Apple push certificate to the Kony Management server. Click +Add to select the certificate from its location and then click Open . The selected certificate with size in KB appears next to push certificate label. |
| Push Certificate Pass Phrase | Enter the password. While accessing, the certificate and the associated password must match. |
| Enterprise Store Provisioning Profile | Using this feature, you can add your Apple enterprise store provisioning profile to the Kony Management server. Click +Add to select the profile from its location and then click Open . The selected profile with size in KB appears next to enterprise store provisioning profile. |

From the iOS Certificates section, you must add two certificates (Distribution and Push) and the Enterprise Store provisioning profile. You can add a Wildcard provisioning profile, optionally. Ensure that you have all the required certificates from your Apple developer account before you start configuring the iOS certificates section.

Configuring Certificates for iOS

To configure certificates for iOS, do the following:

1. In Kony Management admin console, under **Settings**, click **Application Settings**. The Application Settings page opens with the **Certificates** tab open by default.
2. Under **Enterprise Certificates**, click **Plus Add**. The file explorer window opens.
3. Navigate to the location of your enterprise distribution certificate.
4. Select the certificate and then click **Open**. The certificate is added. The selected certificate with size in KB appears next to the Enterprise Distribution Certificate label. The Certificate Pass Phrase field is enabled.
5. Enter the passphrase for the distribution certificate in the **Certificate Pass Phrase** field.

Note: While accessing, the certificate and the associated password must match.

6. If you want to use a wildcard provisioning profile, select the **Use Wildcard Provisioning profile** option. The Wildcard Provisioning Profile option is enabled. (Optional)

Note: Before uploading your app, you should have the distribution certificates for iOS. When the app is ready for publication, you can create wildcard provisioning certificate.

7. Click **Plus Add**. The file explorer window opens.
8. Navigate to the location of your wildcard provisioning profile.

9. Select the provisioning profile and then click **Open**. The profile is added.

Important: The enterprise store app must be in conformance with the certificates uploaded. If the bundle ID prefix for the certificate is `com.XXX.containerapp`, then the bundle ID of the enterprise store must be `com.XXX.containerapp`. It cannot be `com.YYY.containerapp`. If you change the certificates and update the prefix, then you must delete the enterprise store. You must also download on your device a new version of the enterprise store that reflects the updated certificates. For example, in our case, it should be `com.YYY.containerapp`. If you fail to do so, app management features will not work.

Important: You can upload your own mobile provision files for child apps to use. If you use a provisioning profile with a bundle ID `com.xxx.containerapp`, wrapping will fail. Ensure that your child app bundle ID does not contain the text `containerapp`.

10. Under the Enterprise Store Certificates section, click **Plus Add** next to **Push Certificate**. The file explorer window opens.
11. Navigate to the location of your enterprise push certificate.
12. Select the certificate and then click **Open**. The certificate is added. The selected certificate with size in KB appears next to the Enterprise Distribution Certificate label. The Certificate Pass Phrase field is enabled.
13. Enter the passphrase for the push certificate in the **Certificate Pass Phrase** field.

Note: While accessing, the certificate and the associated password must match.

14. Click **Plus Add** next to **Enterprise Store Provisioning Profile**. The file explorer window opens.
15. Navigate to the location of your enterprise store provisioning profile.

16. Select the provisioning profile and then click **Open**. The profile is added.

Once you add all the certificates and provisioning profiles, the **Save** button is enabled.

17. Click **Save** to save the certificates configuration for iOS.

For the distribution certificate and the push certificate, a new Certificate Details button is enabled. Click **Certificate Details** to view the respective certificate details.

Provisioning is the process of preparing and configuring an app to launch on devices. During development, you can designate the devices that can launch. When you submit your app to the store, you just provision your app. Provisioning iOS apps involves the creation of certificates, production, and distribution of provisioning profiles.

6.3.1.2 Android

Google uses various mechanisms to communicate and authenticate with Android apps. Apps are distributed to devices in various ways (through GooglePlay, privately distributed by enterprises, and distributed by a company/developer internally with their teams for testing).

For Android applications, Kony Management uses the following components to communicate with the applications. Specifically, Kony Management uses the following:

- **Google Cloud Messaging:** Using the Google cloud messaging, Kony Management sends to and receives messages from Android applications which are part of the Kony Management suite.
- **Android Keystore System:** Google's Android Keystore mechanism allows a developer to store cryptographic keys in a container. This makes it difficult to extract cryptographic key information from the device.
- **Google Maps API:** Google Maps APIs allow developers to embed Google Maps in Android applications, among other things.

Ensure that you have the following information before you configure the Android certificates:

- A Google developer account
- A project - The project number is used in the **Project Number** field.
- GCM credentials key - The key is used in the **GCM Key** field.
- Google Maps Android API enabled in your project. This key is used in the **API V2 Key** field.

The Android section view displays the following elements:

| Feature | Description |
|----------------------------|---|
| Google ID | Enter your Google developer user name here. You must have a GCM key and a project in this user ID. |
| GCM Key for Android | Enter the Google Cloud Messaging (GCM) Key. For more information on GCM for Android, click here . |
| Project number (Sender ID) | Enter your Google project number or ID here. For more information on how to get your project number, click here . |
| Key Store | Using this feature, you can add your Key store to the Kony Management server. Click +Add to select the key store from its location and then click Open . |
| Key Store Pass Phrase | Enter the required password to access the certificate. |
| Certificate Alias | <p>Enter an alternative name for the certificate.</p> <p>The keystore protects each certificate with its individual password. For example, when you sign an Android application using the Key Store passphrase, you are asked to select a keystore first, and then asked to select a single alias from that keystore. After providing the passwords for both the keystore and the chosen alias, the app is signed and the public key (the certificate) for that alias is embedded into the APK.</p> |

| Feature | Description |
|--------------------------------|---|
| Certificate Pass Phrase | Enter the required password to access the certificate. While accessing, the certificate and the associated password must match. This button is enabled only when a certificate is uploaded to the Kony Management server. |
| Certificate Details | Click this button to view the respective certificate details and associated error, if any. |
| Google Maps Android API V2 Key | Enter your Google Maps Android API V2 key. For information on how to get Google Android API V2 key, click here . |

Android

GCM Key

Google ID

GCM key for Android

Project number (Sender ID)

Key Store Credentials

Key Store debug.keystore

Key Store Pass Phrase

Certificate Alias

Certificate Pass Phrase

Google Maps API

Google Maps Android API V2 Key

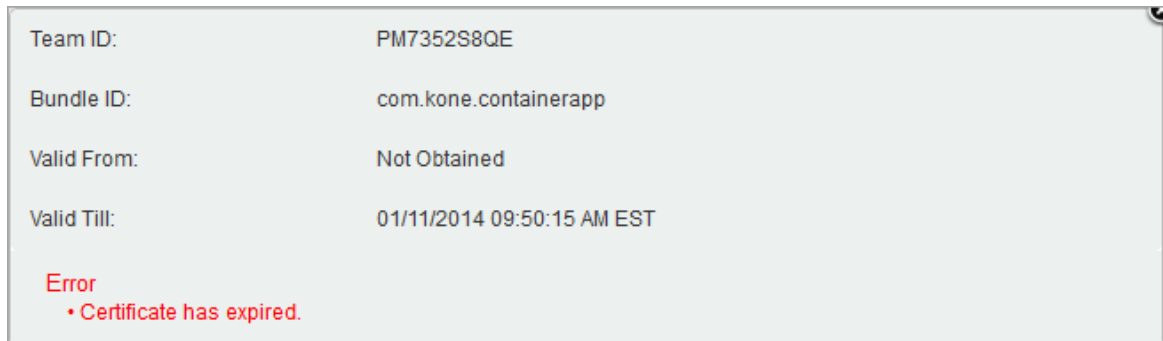
Note Kony will re-sign the Android Launchpad app based on the details provided here. Please click 'Certificate Details' and make sure that the SHA1 fingerprint and the launchpad package name (com.kony.mdmlclient) are appropriately associated with your Google account. In case any Android apps are submitted to EMM and they use Maps, then please make sure the SHA1 fingerprint and application package name are associated to that app's corresponding Google account. The SHA1 fingerprint is replaced as part of the app signing process, hence this task is necessary.

Configuring Certificates for Android

To configure certificates for Android, do the following:

1. In Kony Management admin console, under **Settings**, click **Application Settings**. The Application Settings page opens with **Certificates** tab open by default.
2. In the **Android** section, under the **GCM Key** section, enter details for the following:
 - i. **Google ID/Google ID**: Enter your email account ID.
 - ii. **GCM Key for Android**: Enter your GCM Key for Android.
 - iii. **Project Number (Sender ID)**: Enter the Sender ID.
3. In the **Key Store Credentials** section, enter the following:
 - i. **Key Store**: Click **+Add** to select the certificate from its location and then click **Open**. The selected certificate with size in KB appears next to the Key Store label.
 - a. Click the **Close** icon to close the selected certificate details.
 - ii. **Key Store Pass Phrase**: Enter the required password to access the certificate.
 - iii. **Certificate Alias**: Enter an alternative name for the certificate.

The keystore protects each certificate with its individual password. For example, when you sign an Android application using the Key Store Passphrase, you must select a keystore first, and then select a single alias from that keystore. After providing the passwords for both the keystore and the chosen alias, the app is signed and the public key (the certificate) for that alias is embedded into the APK.
 - iv. **Certificate Pass Phrase**: Enter the required password to access the certificate.



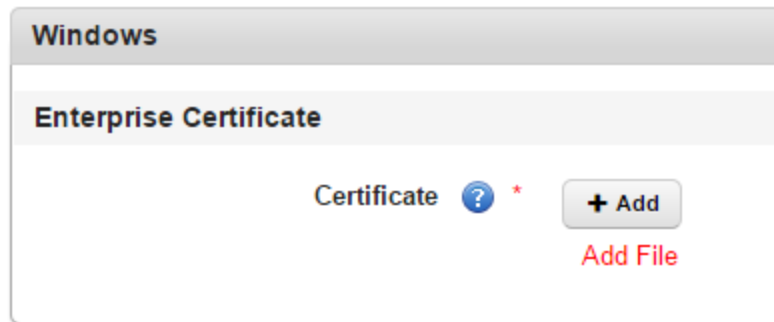
- v. Click **Certificate Details** to view the respective certificate details and associated error, if any.
4. In the **Google Maps API** section, enter the details for the following:
 - i. **Google Maps Android API V2 Key**: Enter the key value for your Google maps Android API.
 5. Click **Save** to save the entered details. In the confirmation message that appears, click **OK** to return to the main page.

6.3.1.3 Windows Phone 8.x

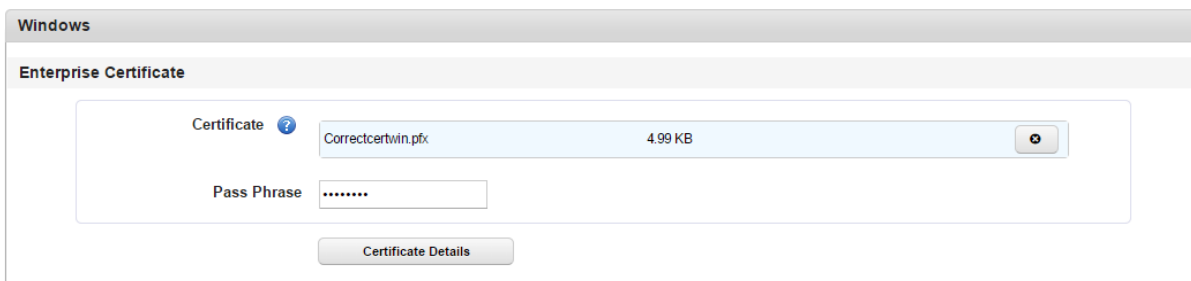
Windows Phone 8.x devices require a Symantec Code Signing Certificate. Symantec is the only provider of code signing certificates for the Windows Phone Private Enterprise program. You can use this certificate to enable and distribute your windows applications within your organization. This certificate ensures that the windows applications are safe to download and for internal distribution in the company.

You must ensure that you have your Symantec enterprise certificate available before you configure this section. For more information on how to obtain this certificate, click [here](#).

To set Certificates for Windows Phone 8.x, follow these steps:



1. **Certificate:** Click **+ Add**. Windows explorer appears.
2. Select your Symantec enterprise certificate and click **Select**.
3. Click **Add**. The certificate is added. The passphrase option appears.
4. Enter your passphrase and click **Save**.



For more information on how to obtain Windows Certificates, see the [Pre-install guide](#).

6.3.1.4 Two-Way SSL Enterprise Certificate

An administrator can configure Kony Management suite to take a system level Two-way SSL certificate and securely bundle the Two-way SSL certificate with the Enterprise Store app.

Important: Two-way SSL feature does not work for the Enterprise Store and child apps for Apple iPad.

Note: If you want the two-way SSL to work on an iPhone, configure the **Kony Fabric Identity service** settings in the **Authentication Settings** page. Specifically, you must configure the **Enable Reverse Proxy Basic Auth** setting.

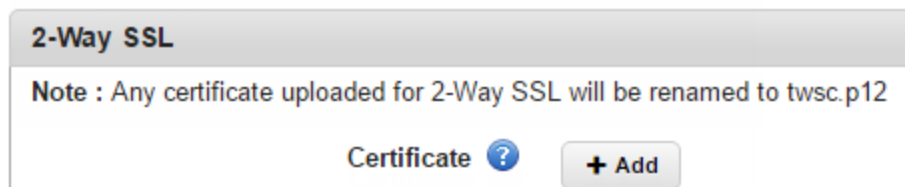
The SSL certificate is used to contact any server resource inside a customer's network that requires mutual authentication - for example, f5 load balancer. You must provide an x509 client side certificate (.p12 supported) for two-way SSL authentication, for the Enterprise Store to authenticate to a back-end. Mutual authentication through two-way SSL allows the client and the server to authorize each other so both parties are assured of each others identities.

See a sample reference for setting up the two-way SSL at <https://support.f5.com/kb/en-us/solutions/public/15000/100/sol15137.html>.

Note: Two-way SSL cert is also be shared with the child app if the **Allow SSO** option is selected during app deployment.

In the Application Settings page, an administrator can upload a two-way SSL certificate.

To upload an enterprise certificate for two-way SSL, follow these steps:



1. **Certificate** : Click **+ Add**. Windows explorer appears.
2. Select your two-way SSL enterprise certificate and click **Select**.
3. Click **Add**. The certificate is added.
4. Click **Save**. A new passphrase field appears.

5. Enter the passphrase associated with the two-way SSL certificate you uploaded in the field.

2-Way SSL

Enterprise Certificate

Certificate ? Sample.p12 5.55 KB ✕

Pass Phrase

Certificate Details

Important: The two-way SSL certificate name must not contain the dot character. For example, if the certificate name is `client.one.p12`, the Kony Management suite administrator console will not save the certificate.

Important: If you upload an incorrect two-way SSL certificate, a user log-in fails in the Enterprise Store.

6.3.2 Usage Settings

The primary purpose of usage settings is to define rules about how a user can log in to web console and devices, session time-out, and invite new users. Usage Settings is divided into the following sections:

- [Login Settings](#)
- [New User Settings](#)
- [Enterprise App Licenses](#)

6.3.2.1 Login Settings

Online Login: This section covers various authentication mechanisms for the Kony Management administrator's console and the Enterprise Store. In this section, you can enable the Captcha feature based on a number of failed attempts, lock a user (from the administrator console or the enterprise store), or even initiate an enterprise wipe on an enrolled device. You can also enable Simple Certificate Enrollment Protocol (SCEP) enrollment for a user. The SCEP enrollment server details are provided at the time of Kony Management suite installation.

Console Settings: In this section, you can configure the idle timeout period for a user in the administrator console.

Offline Login: Using this section, you can configure the maximum failed attempts while the device is offline. If the user exceeds the allowed number of offline login fail attempts, an enterprise wipe is triggered on the device.

Device Limit: Using this section, you can configure the number of devices users can enroll on their user name.

Local EMM User Password Settings: This section allows you to configure password settings for a local EMM user. You can do the following:

- Reset password on the first login
- Configure complexity of passwords
- Configure expiry time period
- Configure re-usage of old passwords

6.3.2.2 New User Settings

Using this section, you can configure imported groups and users settings. You can configure the following settings:

- Whether to overwrite a local user with an imported user
- Whether to overwrite a local group with an imported group

- Syncing groups of Active Directory users after log in
- Creating or importing users without email IDs

6.3.2.3 Authentication Source Configuration

You can use the authentication mechanisms configured in the Authentication Settings page to configure Authentication types for various Kony Management suite interfaces. You can configure authentication for the following:

- Management Admin Console
- Self-service Console
- Enterprise Store download page
- Enterprise Store login

6.3.2.4 Enterprise App Licenses

In this section, you can configure the usage of enterprise licenses. Various settings that you can configure in this section include log in settings, console settings, device limit, local user password settings, new user settings, and enterprise app license settings.

6.3.2.5 User Interface Elements

| Feature | Description |
|---------------------------------------|--|
| Log-in Settings | |
| Require Captcha | The feature allows you to configure the captcha settings. By default, the option is set to Yes . If the selected option is No , then After How Many Failed Attempts field is removed. |
| After How Many Failed Attempts | Select the number of failed attempts a user can have. A Captcha feature will be activated to determine whether a user is human after a user exceeds the number of failed log-in attempts. |

| Feature | Description |
|---|--|
| Lock User After | Select the number of attempts a user can have to log in to the application. A user will be locked after exceeding the allowed number of log-in attempts. This will control access to Enterprise Appstore. However, if the user is locked by the external authentication provider, user will still not be able to log in. |
| Trigger Enterprise Wipe Device After | Select the number of attempts a user can have to log in to the application. After a user exceeds the allowed number of login attempts, all enterprise data will be wiped from the device. After the enterprise wipe, the device will be in the Suspended mode. For Android devices, apps along with app data is removed. App data is removed before uninstalling the app. |
| Enable SCEP Enrollment | Configure the feature to Yes if you want to enable SCEP enrollment on Android devices. When you select Yes, Validate Client Certificate option is enabled. |
| Validate client Certificate (OCSP Revocation Checking) | By default, the setting is set to No . If you want to validate the client certificate, select Yes . The OCSP URL field is enabled. For more information on OCSP URL configuration, click here . |
| OCSP URL | Enter the OCSP URL in the field to validate the client certificate. |
| Notify User Before SCEP CA expire | Select the number of days from the list. Based on this setting, users will be informed for the specified number of days about the certificate expiration before the certificate expire date. |
| Console settings | |
| Console Idle Timeout Period | Select the timeout period for the console in minutes. After the limit is reached, the user must log in online to access the administrator console again. |
| Offline Login | |

| Feature | Description |
|--|---|
| Maximum Failed Attempts Offline | <p>Select the number of attempts a user can have to login offline to enterprise store. After the limit is reached, the User must log in online to access enterprise store again.</p> <p>For Android devices, if the user exceeds the maximum number of allowed attempts, enterprise wipe will be initiated on the device.</p> |
| Trigger Enterprise Wipe on Device after Failed Attempts Offline | <p>Select the number of attempts a user can have to log in to the application. After a user exceeds the allowed number of login attempts, apps along with app data is removed. App data is removed before uninstalling the app. This is applicable only for Android devices.</p> |
| Device Limit | |
| Maximum number of Devices Per User | <p>Admin can limit the number of devices per user to be registered. Select one of the options from the list. Once the limit is reached, all subsequent device registrations will fail.</p> |
| Local EMM User Password Settings | |
| Reset Password on First Log-in | <p>Configure this to Yes to force a user to reset the password on the first log in. This feature is not applicable on the Management console. The Reset password feature is applicable for the enterprise store and the self-service console.</p> |

| Feature | Description |
|--|--|
| Complexity of Password | <p>Select the complexity of the password from the list. Options are Any, Numeric, Alphanumeric, Alphabetic, and Complex. When you select Complex, the following fields appear.</p> <p>For all these fields, you can select a minimum number of characters for each one of these fields. Based on your selection, the criteria for the complex password will be set.</p> <ul style="list-style-type: none"> i. Minimum Number of Letters ii. Minimum Number of Lowercase Letters iii. Minimum Number of Uppercase Letters iv. Minimum Number of Non-letters v. Minimum Number of Numeric Digits vi. Minimum Number of Symbols |
| Minimum Length of Password | Select the minimum length of the password from the list. |
| Expires in | Select an option from the list. Options are Never and Custom . When you select Custom , a new field Days is available. Enter the number of days after which, the password must expire. |
| Unique Password Required Before Reuse | Using this field, you can restrict the reuse of a password. The user will not be allowed to reuse a password before a specific period. The available range is from one to ten. |
| New User Settings | |

| Feature | Description |
|--|--|
| Overwrite Local User with Imported User | By default, this option is set to No . If you want to overwrite a local user with the first imported user, click Yes . It will overwrite only if the user name is present in the local directory. |
| Overwrite Local Group with Imported Group | By default, this option is set to No . If you want to overwrite a local group with the first imported group, click Yes . It will overwrite only if the group name is present in the local directory. |
| Sync Groups for AD Users After Login | By default, this option is set to Yes . If you do not want to sync groups for active directory users after login, select No . |
| Create/Import Users Without Email | By default, this option is configured to No. If configured to Yes, users can be created/imported into the EMM server without an email ID from both Active Directory and locally. For a user imported without an email address: <ol style="list-style-type: none"> <li data-bbox="597 1079 1377 1157">1. Email notifications cannot be sent to the user. These notifications include user enrollment, device actions, app updates, and others. <li data-bbox="597 1194 1008 1230">2. Email policies cannot be applied. <li data-bbox="597 1268 1295 1346">3. The user cannot participate in the iOS Volume Purchasing Program. |

| Feature | Description |
|--|--|
| | <p>You must be very cautious when enabling the Create/Import Users Without Email feature. For a super administrator, if the email address is empty (because the Create/Import Users Without Email feature is set to Yes), then the super administrator will not receive email notifications for the following:</p> <ul style="list-style-type: none"> • Notifications on expiring certificates (Android Key Store, APNs certificate, iOS Enterprise Distribution Certificate, iOS push certificate, MDM vendor Signing certificate, SCEP certificate, SSL certificate, Windows Enterprise Certificates) • Notifications on expiring iOS provision profiles (Enterprise and store provisioning profiles) • Device Compliance violations • Reset Password information • Enrollment confirmation and failure emails • Exchange Service Settings failure emails <p>A user with limited administrator permissions will not get Reset password information notifications.</p> |
| | <p>Enterprise App Licenses</p> |
| <p>Enable Enterprise App Licenses</p> | <p>By default, this is set to No. Configuring this to Yes will enable restricting enterprise app distribution through licenses.</p> |

6.3.2.6 How to Configure Captcha Settings

Using the captcha feature, you can enforce extra security in the user log-in process. You can specify the number of failed attempts after which you can lock a user, wipe a device, etc.

To enable Captcha settings while logging into the management administrator console and the Enterprise store, follow the steps below:

1. In Kony Management admin console, under **Settings**, click **Application Settings**. The Application Settings page opens with the Certificates tab open by default.
2. Under **Login Settings**, for the **Require Captcha** field, select **Yes**. New fields appear.
3. From the **Display Captcha after** list, select the number of allowed failed login attempts. For example, 3.
4. To lock the user after the allowed number of failed login attempts, from **Lock User** list, select an option. For example, Custom. A field appears next to the list. Provide a value from 1 to 30.
5. From the **Trigger Enterprise Wipe on Device after** field, select **Custom**. A field appears next to the list. Provide a value from 1 to 30.
6. Click **Save**. A success message appears.
7. Click **OK**. Your captcha settings are saved.

Important: The captcha is displayed only when login attempts fail (based on login settings) to a device-user enrolled with the EMM server. For a user not enrolled with the EMM server, the captcha is not displayed. In such scenario, the system displays the generic warning message that the device is enrolled with another user.

6.3.2.7 How to Configure SCEP Enrollment

Simple Certificate Enrollment Protocol (SCEP) helps a user to request their digital certificate electronically to authenticate their identity.

To configure SCEP Enrollment settings, follow the steps below:

1. In Kony Management admin console, under **Settings**, click **Application Settings**. The Application Settings page opens with the Certificates tab open by default.
2. Click the **Usage Settings** tab. The usage Settings page appears.

3. Under the Login Settings, from the **Enable SCEP Enrollment** select **Yes**. This is applicable only for Android devices.
4. Click **Save**. A confirmation message appears.
5. Click **OK**. Your SCEP enrollment settings are saved.

6.3.2.8 How to Configure Console Idle Timeout Period

Using the console idle timeout feature, you can force a user to log in to Kony Management administrator console after a specified time period.

To configure Console Idle Timeout period settings for the management administrator console, follow the steps below:

1. In Kony Management admin console, under **Settings**, click **Application Settings**. The Application Settings page opens with the Certificates tab open by default.
2. Click the **Usage Settings** tab. The Usage Settings page appears.
3. Under the **Login Settings**, from the **Console Idle Timeout Period** list, select the number of minutes after which the admin console will log out a user if the user has been idle.
4. Click **Save**. A success message appears.
5. Click **OK**. Your console idle timeout settings are saved.

6.3.2.9 How to Configure Offline Login settings

To configure Console offline login period settings for the management administrator console, follow the steps below:

1. In Kony Management admin console, under **Settings**, click **Application Settings**. The Application Settings page opens with the Certificates tab open by default.
2. Click the **Usage Settings** tab. The Usage Settings page appears.

3. Under the **Login Settings**, from the **Offline Login** section, select an option from the **Maximum Failed Attempts Offline** list. If you select **Custom**, a new text box appears. Enter a number in it.

Note: After the limit is reached, the user must log in online to access the Enterprise Store again.

4. If you want to trigger enterprise wipe on a device after exceeding the allowed failed attempts offline, select **Yes** for the **Trigger Enterprise Wipe on Device after Failed Attempts Offline** field.

Note: This feature is available only on Android devices.

5. Click **Save**. A success message appears.
6. Click **OK**. Your offline login settings are saved.

6.3.2.10 How to Configure Device Limit for a User

To configure the number of devices allowed for a user to enroll, follow the steps below:

1. In Kony Management admin console, under **Settings**, click **Application Settings**. The Application Settings page opens with the Certificates tab open by default.
2. Click the **Usage Settings** tab. The Usage Settings page appears.
3. Under **Login Settings**, from **Device Limit** section, select an option from the **Maximum Number of devices per user** list. If you select unlimited, users can enroll any number of devices.
4. Click **Save**. A success message appears.
5. Click **OK**. Your device limit settings are saved.

6.3.2.11 How to Configure Local EMM User Password Settings

To configure local Kony Management user password, follow the steps below:

In this example, we will create a complex password that needs to be reset at the first login, which expires in 30 days and the number of unique passwords before using an old password is three.

1. In Kony Management admin console, under **Settings**, click **Application Settings**. The Application Settings page opens with the Certificates tab open by default.
2. Click the **Usage Settings** tab. The Usage Settings page appears.
3. Under **Local EMM User Password settings**, configure **Reset password on the first login to Yes**.
4. From the **Complexity of password** list, select **Complex**. New fields appear.
5. From the **Minimum length of password** list, select **8**.
6. From the **Minimum Number of Letters** list, select **2**.
7. From the **Minimum Number of Lower Case Letters** list, select **1**.
8. From the **Minimum Number of Upper Case Letters** list, select **1**.
9. From the **Minimum Number of Non-Letters** list, select **1**.
10. From the **Minimum Number of Numeric Digits** list, select **1**.
11. From the **Minimum Number of Symbols** list, select **1**.
12. From the **Expires in** list, select **Custom**. In the new text box that appears, enter 30. This is in days.
13. From the **Unique Password required before reuse** list, select **3**.
14. Click **Save**. A success message appears.
15. Click **OK**. Your EMM local user password settings are saved.

6.3.2.12 How to Configure New User Settings

To configure New User settings, follow the steps below:

1. In Kony Management admin console, under **Settings**, click **Application Settings**. The Application Settings page opens with the Certificates tab open by default.
2. Click the **Usage Settings** tab. The Usage Settings page appears.
3. Under **New User Settings**, select an option for the following fields:
 - i. Overwrite Local User with Imported User. If this is configured to yes, the local user with the same name will be overwritten with the imported user.
 - ii. Overwrite Local Group with Imported Group. If this is configured to yes, the local group will get overwritten with the first imported group.
 - iii. Sync Groups for AD Users after Login. If this is configured to yes,
 - iv. Create/Import users without email ID. If this is configured to yes, users can be created without an email ID from Microsoft Active Directory and locally. For Users created/imported without email addresses, email notifications cannot be sent (This includes Enrollment, Device Actions, App Updates). Email policy cannot be applied. The user cannot participate in VPP.
4. Click **Save**. A success message appears.
5. Click **OK**. Your new user settings are saved.

6.3.2.13 How to Configure Authentication Source

To configure Authentication Source, follow the steps below:

1. In Kony Management admin console, under **Settings**, click **Application Settings**. The Application Settings page opens with Certificates tab open by default.
2. Click **Usage Settings** tab. Usage Settings page appears.
3. Under Authentication Source Configuration, select an option for the following fields from the drop down list. If you have configured any authentication mechanisms in your Authentication Settings page, they will appear in the list.

- i. Management Console
 - ii. Self Service Console
 - iii. Enterprise Store Download Page
 - iv. Enterprise Store Login
4. Click **Save**. A success message appears.
 5. Click **OK**. Your new user settings are saved.

Once set, your respective login screen will take you to the configured authentication page.

6.3.2.14 How to Configure Enterprise App Licenses

To configure Enterprise App Licenses, follow the steps below:

1. In Kony Management admin console, under **Settings**, click **Application Settings**. The Application Settings page opens with the Certificates tab open by default.
2. Click the **Usage Settings** tab. The Usage Settings page appears.
3. Under the Enterprise App Licenses heading, select **Yes** for **Enable Enterprise App Licenses**.
4. Click **Save**. A success message appears.
5. Click **OK**. Your Enterprise App license settings are saved.

6.3.3 Error Messages

Error Messages tab contains various pre-defined error message areas, where an administrator can enter appropriate messages that can be shown to an end user when an error occurs. The Administrator is expected to specify the messages for each of these situations.

The **Error Messages** tab includes the following sections:

- Network Permission Error Messages
- Device Storage Error Messages
- Clip Board Error Messages
- Application Features Error Messages
- Phone Features Error Messages
- Direct and offline app launch Messages

Network Permission Error Messages

| Network Permission error messages | |
|---|---|
| Network communication is not allowed | Policy violation. Network Access not allowed |
| Specified network domain is not allowed | Policy violation. Specified domain not allowed |
| Network access through WI-FI is not allowed | Policy violation. Network Access through wi-fi not allowed |
| Network access through current active WI-FI is not allowed | Policy violation. Network Access not allowed for the currently active wi-fi |

1. Enter the customized error messages for the following fields:
 - a. Network Communication is not Allowed
 - b. Specified Network Domain is not Allowed
 - c. Network Access through Wi-Fi is not Allowed
 - d. Network Access through Current Active Wi-Fi is not Allowed

Device Storage Error Messages

Device Storage error messages

External Secure Digital card read access is not allowed

Policy violation. External rea

External Secure Digital card write access is not allowed

Policy violation. External wri

2. Enter the customized error messages for the following fields:
 - a. External Secure Digital Card Read Access is not Allowed
 - b. External Secure Digital Card Write Access is not Allowed

Clip Board Error Messages**Clip board error messages**

"Cut" "Copy" & "Paste" operation is not allowed

Policy violation. Cut not allo

3. Enter the customized error messages for the following field:
 - a. Cut Copy and Paste operation is not allowed.

Application Features Error Messages

| Application Features error messages | |
|--|--|
| Document sharing from the application is not allowed | Policy violation. Document sharing not allowed |
| Application idle time out | |
| Application launch after expiry date | App Expired |
| Application is used in non-business hours | Business Hour Expired |
| Application is used in non-business days | |
| Application is used in non-designated location | App running outside App region |
| Application is locked and is inaccessible | App Locked |

4. Enter the customized error messages for the following fields:
 - a. Document sharing from the application is not allowed
 - b. Application idle timeout
 - c. Application launch after expiry date
 - d. Application is used in non-business hours
 - e. Application is used in non-business days
 - f. Application is used in non-designated location
 - g. Application is locked and is inaccessible

Phone Features Error Messages

| Phone feature error messages | |
|---|---------------------------------|
| Usage of SMS is not allowed | Policy violation. SMS Acces |
| SMS to the specified number(s) is not allowed | Policy violation. SMS to this |
| Email usage is not allowed within the Application | Policy violation. Email Acce |
| Email to the specified email address(es) is not allowed | Policy violation. Email to thi: |
| Phone dialer access is not allowed | Policy violation. Phone Acce |
| Phone call for specified number(s) is not allowed | Policy violation. Phone call t |
| Camera access is not allowed | Policy violation. Camera Acc |

5. Enter the customized error messages for the following fields:

- a. Usage of SMS is not allowed
- b. SMS to the specified number(s) is not allowed
- c. Email usage is not allowed within the application
- d. Email to the specified email address (es) is not allowed
- e. Phone dialer access is not allowed
- f. Phone call for specified number(s) is not allowed
- g. Camera access is not allowed

Direct and Offline App Launch

Direct and offline app launch

| | |
|---|---|
| App Launch Restricted | <input type="text"/> |
| App Launch Restricted Offline | <input type="text" value="device is offline"/> |
| Offline Authentication Failure Limit | <input type="text" value="You may no longer use Launchpad offline. Please try to login while online"/> |
| Offline Access for Messages | <input type="text" value="Cannot Access Messages You must connect to a Wi-Fi or mobile data network to access Messages"/> |
| Launchpad Deleted | <input type="text" value="Launchpad must be installed on device, otherwise you cannot launch any enterprise apps"/> |

Note: The error messages are shown to the user on device for Policy violations

1. Enter the customized error messages for the following fields:
 - a. App Launch Restricted
 - b. App Launch Restricted Offline
 - c. Offline Authentication Failure Limit
 - d. Offline Access for Messages
 - e. Enterprise Store Deleted

6.3.4 Encryption Key

If an app that uses SQLite database is not encrypted, the app is prone to security threats when the device is lost, rooted, or jailbroken. To ensure that the SQLite database is secure, the database is encrypted with a key for security. An encryption key helps an app protect the security of digital data.

Prior to Kony Management 3.5 release, an administrator could generate an encryption key directly, and the user could specify the key. However, with the 3.5 release, Kony Management assumes the task of generating a unique encryption key for each app installed on any device. This change helps an administrator to automate and schedule encryption key generation.

When a new key is generated, all wrap and sign child apps are re-wrapped, including the enterprise store, and a user must upgrade all apps. If the schedule is left blank, the PKI key pairs are generated when the administrator provides the app signing certificates. These PKI key pairs continue to be used unless the administrator generates a new PKI key pair using the **Generate Now** button.

Application Settings

Certificates
Usage Settings
Error Messages
Encryption Key
VPP Apps
Message Templates

Note :Wrap and Sign job would be triggered for all the Enterprise Apps, every time a new PKI key pair is generated.

Generate Keys

Note : The encryption keys are generated automatically. The below schedule is to generate the PKI key pair to protect the encryption keys.

Schedule: Yearly Monthly

The Second Tuesday of February for every 1 years from 2015

Every March on day 0 for every 1 years from 2015

Start Time (In 24-hour format): 1 : 1

Schedule

Status

| Platform | Last Key Generated On | Next Key Generation Scheduled On |
|----------|---------------------------|----------------------------------|
| Android | 11 May, 2015 07:30:27 EDT | 09 Feb, 2016 02:01:00 EDT |
| iOS | 12 May, 2015 08:40:18 EDT | 09 Feb, 2016 02:01:00 EDT |

Generate Now

The Encryption Key tab has the following fields:

- **Generate Keys:** You can set the encryption key schedule in this section.
 - **Schedule:** You can set the encryption key generation yearly or monthly.
 - **Yearly**
 - **The:** This field contains five lists. The first list has four options: First, Second, Third, and Fourth. The second lists weekdays. The third lists months. You can enter the number of years in the fourth list. The fifth lists years. An example of this schedule is: The **Second Tuesday** of **February** for every **2**

years from **2015**.

- **Every:** This field contains four lists. The first list has all months. The second list is a day list. You can enter the number of years in the third list. The fourth lists years. An example of this schedule is: Every **February** on day **10** for every **4** years from **2015**.
- **Monthly**
 - **The:** This field contains two drop-down lists and one text field. The first list has four options: First, Second, Third, and Fourth. The second lists weekdays. You can enter the month interval in the text field. An example of this schedule is: The **Second Tuesday** of every **2** month (s).
 - **Day:** This field contains two text fields. The first one is for a day and the second one is for months. An example of this schedule is: Day **10** of every **3** month(s).
- **Start Time:** The start time field contains two lists. The first list contains the number of hours, and the second one is for minutes.
- **Schedule:** Clicking this button will schedule the encryption key generation.
- **Status:** This section displays information on existing encryption key details for various platforms:
 - **Platform:** Displays the platform name.
 - **Last Key Generated On:** Displays the time the encryption key was generated.
 - **Next Key Generation Scheduled On:** Displays the time when the next key generation is scheduled.
 - **Generate Now:** Click this button to generate a PKI pair for iOS and Android immediately.

6.3.5 VPP Apps (VPP for iOS 7+ devices)

The VPP Apps tab is used to configure VPP settings for iOS 7+ devices.

The screenshot shows the 'VPP Apps' configuration window. It contains the following elements:

- Apple ID *
- Token *
- Applist Sync *
- Last Sync: Not Synced
- Save

To create a VPP, the admin must register to Apple's VPP and procure a token. A VPP Program Facilitator can obtain a token by logging into the appropriate VPP website.

- For Business customers: <https://vpp.itunes.apple.com/>

Currently, Kony Management supports Apple's VPP for Business customers only through Managed distribution method.

6.3.5.1 Configuring VPP Settings

To configure VPP settings, follow these steps:

1. Enter the Apple ID to run the VPP.

An Apple ID that is used for creating a VPP is different from a Developer Apple ID or an Apple Device ID. A user should have a separate Apple ID to create a VPP. Developer IDs are either individual or corporate. These IDs are not supported to create a VPP.

2. Enter the token ID provided by Apple.

For Business customers, the Token is generated by logging into <https://vpp.itunes.apple.com/>

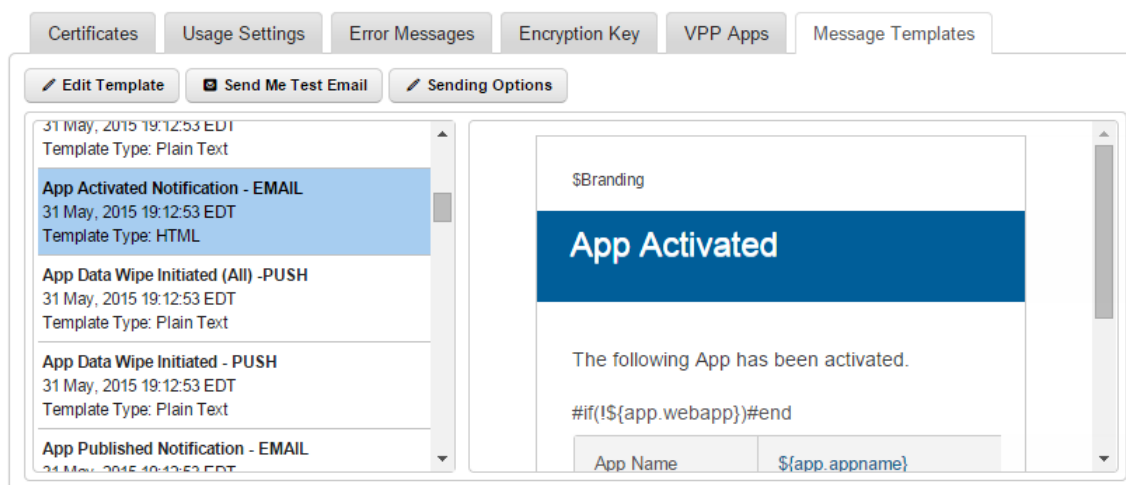
Each token is valid for one year from the time it is generated.

3. In **Applist Sync**, select one of the time periods from the list to sync the latest list of purchased apps, VPP enrollment status, and licenses distributed. Based on the sync time, the system syncs with the Apple server and gets the latest status. You can configure one of the following:
 - 1 hour
 - 3 hours
 - 6 hours
 - 12 hours
 - 24 hours
4. **Last Sync**: Displays the last sync date and time details. Click the **Sync Now** button to start the sync immediately to sync the purchased app list and licenses distributed with EMM.
5. Click **Save** to save the settings.

Once the sync completed, the VPP apps page is updated in the [App Management > VPP Apps](#) page.

6.3.6 Message Templates

The Message Templates tab displays a list of all messages (Push and Email) that an administrator can send to users.



The Message Template tab displays the following fields:

- **Edit Template:** You can use this button to edit existing message templates.
- **Send Me Test Email:** You can send yourself a test email of any message template of your choice to view how the message template looks. Especially when you made any modifications to an existing template format.
- **Sending Options:** You can customize sending options for each of the message template based on the required audience. Some messages are specific to affected users, some can be specific to administrators, and some can affect all users. Using this button, you can choose the recipients of any given template.

Email messages can be of two types:

- Plain Text
- HTML

Push Messages are always plain text only.

Important: Do not modify the placeholders as fetching data required could fail. Ensure that you verify the changes to the HTML template before finalizing the template.

6.3.6.1 Pre-Defined Templates

The system provides pre-defined message templates for all known situations that help an administrator to create custom messages. Message templates have placeholders of various nouns from App Management. An administrator can also modify these message templates if required.

6.3.6.2 Editing a Template

The Admin can edit pre-defined templates. The placeholder tags must not be modified, but can be shifted from one place to another. If tags are modified, the system can not fetch the data for that tag. Ensure that you only modify tags labels if required.

For example:

| Tag Labels | Placeholders |
|------------|-------------------------------|
| App Name | <code>\${app.appname}</code> |
| Version | <code>\${app.version}</code> |
| Category | <code>\${app.category}</code> |
| Platform | <code>\${app.platform}</code> |

To edit a template, follow these steps:

1. Click the **Edit Template** button. The system displays the **Edit Template** dialog.

Edit Template [X]

Template Name * App Published Notification - EMAIL

Template Medium Email Push Notification

Message Box :*

Branding Logo

App Published

The following App has been published and will be available in EMM Store

| | |
|----------|-----------------|
| App Name | \${app.appname} |
| Version | \${app.version} |

Disclaimer: Existing place holders can be duplicated or relocated within the template or removed. No new place holders will be supported. Ensure you verify the changes to the HTML template before finalizing the template.

2. Select either the Email or Push Notification as a **Template Medium**.
3. Click in the **Message Box** area to make any necessary changes instantly if required.

There are two views that you can use when editing – HTML View (WYSIWYG) and Source View.

You can switch between the views by clicking the **HTML View** and **Source View** buttons.

4. Click **Save** to save the changes.

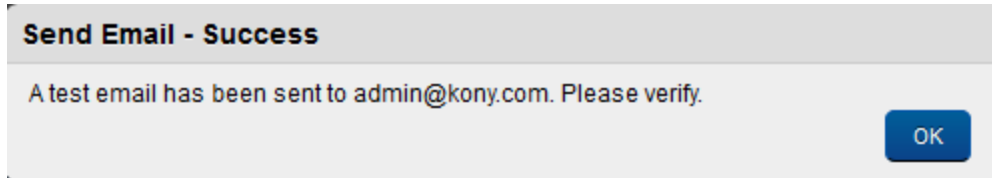
6.3.6.3 Sending a Test Email

Admin can preview and test HTML emails before sending them out to users.

To send a test mail, follow these steps:

1. Click the **Sending Me Test Email** button.

The system displays sent email success message "A test email has been sent to *admin@kony.com*. Please verify."



2. Click **OK** to confirm the same. The email will be sent to admin who currently logged into the EMM console.

6.3.6.4 Configuring Sending Options

This feature helps you enable or disable message-template notifications to users. If you send notifications, you can customize the audience for these notifications. You can customize sending options for each message templates based on the required audience. Messages can be specific to affected users, administrators, or all users.

Sending Options

The Sending Options window displays the following fields:

- **Template Name:** This field displays the message template name.
- **Enable Sending Email:** Select **Yes** to enable the **Sending Email** feature. The To, Cc, and Bcc fields are enabled when you select Yes. Select **No** to disable the **Sending Email** feature.
- **To:** Select the user who will receive the email. Options are Affected User and Email Admin.
- **Cc:** Select the user you want to copy when you send the email to a recipient. Options available are Affected User and Email Admin.

- **Bcc:** Select the user you want to blind carbon copy when you send the email to a recipient. Options are Affected User and Email Admin.
- **Save:** Click to save the changes you made.
- **Cancel:** Click to cancel the changes you made.

The screenshot shows a dialog box titled "Sending Options" with a close button (x) in the top right corner. The dialog contains the following elements:

- Template Name:** Agent Download Notification - EMAIL
- Enable Sending Email:** Radio buttons for **Yes** (selected) and **No**.
- To:** A dropdown menu with "Affected User" selected.
- Cc:** A dropdown menu with "Email Admin" selected.
- Bcc:** A dropdown menu with "Email Admin" selected.
- Buttons:** "Save" and "Cancel" buttons at the bottom.

To configure Sending Options,

1. Click **Sending Options**. The Sending Options dialog appears.
2. From **Enable Sending Email**, select **Yes**.
3. In the **To** field, select the user who will receive the email. Options are Affected User and Email Admin.
4. In the **Cc** field, select the user you want to copy when you send an email to a recipient. Options are Affected User and Email Admin.
5. In the **Bcc** field, select the user you want to blind carbon copy when you send an email to a recipient. Options are Affected User and Email Admin.
6. Click **Save** to save the changes you made. A success message appears.
7. Click **OK**.

6.3.6.5 Deleting a Template

An administrator can not delete pre-defined templates.

6.4 Admin Email Settings

Admin Email Settings allows an administrator to set the preferences relating to how emails are sent. These settings control how emails are generally sent by the system.

From the **Settings** section, click **Admin Email Settings** on the left panel. The Admin Email Settings page appears.

Admin Email Settings

Admin Email Settings

Host Name*

Port*

Sender Email*

Sender Display Name*

Connection Security*

Authentication required Yes No

Authentication Email*

Authentication Password

To configure Admin Email Settings, follow these steps:

1. **Host Name:** Enter your host name.

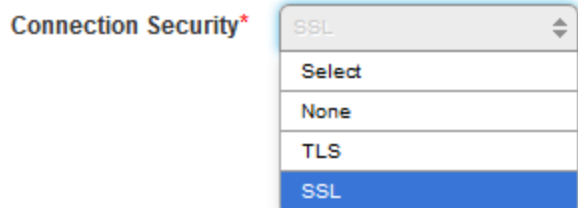
Hostname is the domain name that absolutely and uniquely identifies every computer hooked up to the Internet through the Domain Name Service (DNS) naming hierarchy. You use host name to communicate with the registered devices to EMM.

2. **Port:** Enter your port number.

Port Number is part of the addressing information. It is used to identify the senders and receivers of the message.

3. **Sender Email:** Enter your email address to communicate with devices.

4. **Sender Display Name:** Enter a user-friendly display name. Sender Display Name is associated with the Sender Email address.



5. **Connection Security:** Select the required option from the drop-down list.
6. **Authentication Required:** By default, this option is set to **No**. If you select the option as **Yes**, then Authentication Email and Authentication Password fields become active.
7. **Authentication Email:** Enter your authentication email. You can also enter your user name to authenticate sender's email.
8. **Authentication Password:** Enter your authentication password.
9. Click the **Validate Email** button.

The System verifies the entered details and displays the confirmation message.

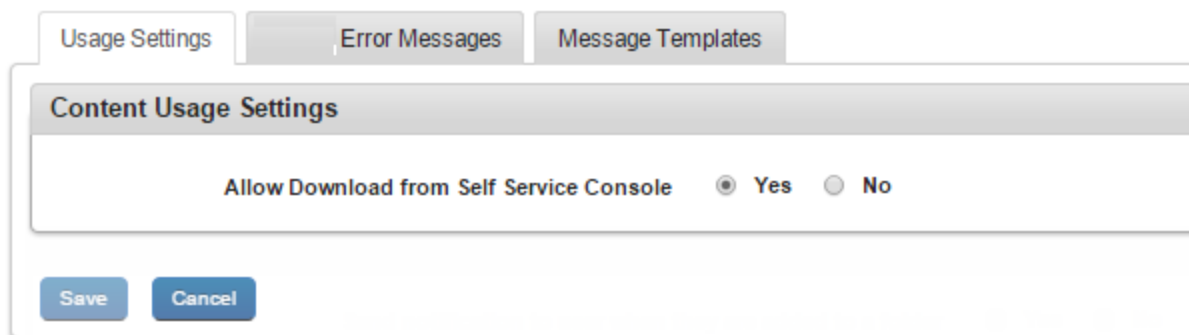
10. Click the **Save** button. In the confirmation message that appears, click **OK** to continue.

11. Click the **Delete** button to delete the existing settings. The System displays the warning message (Delete Admin Email Settings) asking, if a user really wishes to delete the Admin Email Settings?
12. Click **Yes** to continue.
13. In the success message that appears, click **OK** to return to the main page. The deleted Admin Email Settings is removed.

6.5 Content Settings

Use the content settings to manage general settings and better meet the needs of the content you are creating. The Content settings include Usage Settings, Message Templates, and Error Messages.

Content Settings



The screenshot shows a dialog box titled "Content Usage Settings" with three tabs: "Usage Settings", "Error Messages", and "Message Templates". The "Usage Settings" tab is active. Inside the dialog, there is a section labeled "Content Usage Settings" containing the setting "Allow Download from Self Service Console" with two radio buttons: "Yes" (selected) and "No". At the bottom of the dialog are "Save" and "Cancel" buttons.

Usage Settings: You can configure usage settings and notification settings for content.

- **Allow Download from Self Service Console:** By default, this is set to **No**. You can change this to **Yes**.

Usage Settings Error Messages Message Templates

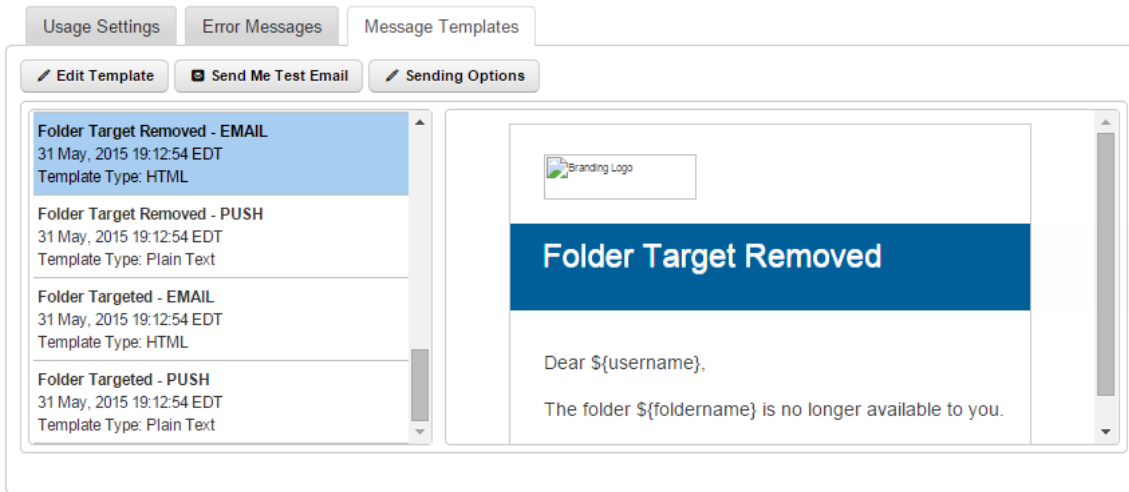
Policy Error Messages

| | |
|-------------------|---|
| Document Expired | <input type="text" value="modified message for document expiry"/> You have 485 characters left |
| Out of Geo-Fence | <input type="text" value="modified message for out of geo-fence"/> You have 483 characters left |
| Out of Time Fence | <input type="text" value="modified message for out of time fence"/> You have 483 characters left |

Save Cancel

Error Messages: Displays available policy error messages in the system. For each of the policy, you can add customized error text message. The following are the available policies. You can add upto 500 characters.

- Document Expired
- Out of Geo-Fence
- Out of Time Fence



Message Templates: Message Templates tab displays available message templates. You can edit an existing template and also send a test mail to yourself with the edited template text.

- [Edit Template](#)
- [Send Me Test Mail](#)
- [Sending Options](#)

6.5.0.1 Editing a Template

The Admin can edit pre-defined templates. The placeholder tags must not be modified, but can be shifted from one place to another. If tags are modified, the system can not fetch the data for that tag. Ensure that you only modify tags labels if required.

To edit a template, follow these steps:

1. Click the **Edit Template** button. The system displays the **Edit Template** dialog.
2. Select either the Email or Push Notification as a **Template Medium**.
3. Click in the **Message Box** area to make any necessary changes instantly if required.

There are two views that you can use when editing – HTML View (WYSIWYG) and Source

View.

You can switch between the views by clicking the **HTML View** and **Source View** buttons.

4. Click **Save** to save the changes.

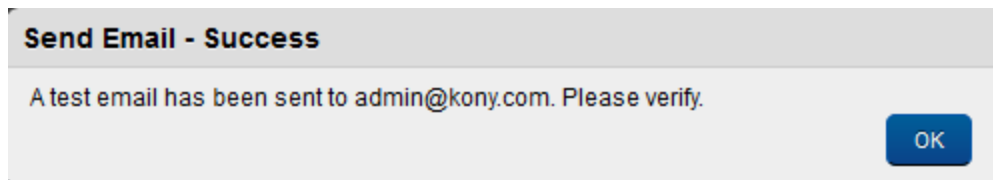
6.5.0.2 Sending a Test Email

Admin can preview and test HTML emails before sending them out to users.

To send a test mail, follow these steps:

1. Click the **Sending Me Test Email** button.

The system displays sent email success message "*A test email has been sent to admin@kony.com. Please verify.*"



2. Click **OK** to confirm the same. The email will be sent to admin who currently logged into the EMM console.

6.5.0.3 Configuring Sending Options

This feature helps you enable or disable message-template notifications to users. If you send notifications, you can customize the audience for these notifications. You can customize sending options for each message templates based on the required audience. Messages can be specific to affected users, administrators, or all users.

Sending Options

The Sending Options window displays the following fields:

- **Template Name:** This field displays the message template name.
- **Enable Sending Email:** Select **Yes** to enable the **Sending Email** feature. The **To**, **Cc** and **Bcc** fields are enabled when you select **Yes**. Select **No** to disable the **Sending Email** feature.
- **To:** Select the user who will receive the email. Options are **Affected User** and **Email Admin**.
- **Cc:** Select the user you want to copy when you send the email to a recipient. Options available are **Affected User** and **Email Admin**.
- **Bcc:** Select the user you want to blind carbon copy when you send the email to a recipient. Options are **Affected User** and **Email Admin**.
- **Save:** Click to save the changes you made.
- **Cancel:** Click to cancel the changes you made.

The screenshot shows a dialog box titled "Sending Options" with a close button "x" in the top right corner. The dialog contains the following fields and controls:

- Template Name:** Agent Download Notification - EMAIL
- Enable Sending Email:** Radio buttons for **Yes** (selected) and **No**.
- To:** A dropdown menu with "Affected User" selected.
- Cc:** A dropdown menu with "Email Admin" selected.
- Bcc:** A dropdown menu with "Email Admin" selected.
- Buttons:** "Save" and "Cancel" buttons at the bottom.

To configure Sending Options,

1. Click **Sending Options**. The Sending Options dialog appears.
2. From **Enable Sending Email**, select **Yes**.
3. In the **To** field, select the user who will receive the email. Options are **Affected User**, and **Email Admin**.

4. In the **Cc** field, select the user you want to copy when you send an email to a recipient. Options are Affected User, and Email Admin.
5. In the **Bcc** field, select the user you want to blind carbon copy when you send an email to a recipient. Options are Affected User and Email Admin.
6. Click **Save** to save the changes you made. A success message appears.
7. Click **OK**.

6.6 Custom Attribute Sets

The Custom Attribute Sets feature allows an administrator to add new attributes to a user whom an administrator can access in an enterprise app through a query. Using a custom attribute set, an app developer can customize the experience of an app targeted to a user. You can do the following:

- Create Custom Attribute Sets
- Apply custom attribute sets for a user
- Apply custom attribute sets for a group
- Apply custom attribute sets for an app
- Apply custom attribute sets for a device

An administrator can create a new custom attribute set and add custom attributes for an enterprise app, specifically targeted to a user, a group, an app, and a device.

Note: There are no restrictions on custom attribute set name or attributes. A custom attribute set can be empty and repeated. As custom attribute sets are defined by an app developer, the app developer must take care of names and values.

Custom Attribute Sets

[+ New CustomAttribute Set](#)

 Displaying 1 - 4 of 4 - Display

| <input type="checkbox"/> | Custom Attribute Set | Description | Last Modified by | Last Modified on | Actions |
|--------------------------|---|---|----------------------------------|---------------------------|--|
| | <input type="text" value="Search Custom Attributes"/> | <input type="text" value="Search Description"/> | <input type="text" value="All"/> | | |
| <input type="checkbox"/> | Star Fleet | | admin | 11 Mar, 2015 03:18:02 EDT | <input type="text" value="Select Action"/> |
| <input type="checkbox"/> | Finance Team | | admin | 11 Mar, 2015 03:17:48 EDT | <input type="text" value="Select Action"/> |
| <input type="checkbox"/> | Management | | admin | 11 Mar, 2015 03:17:30 EDT | <input type="text" value="Select Action"/> |
| <input type="checkbox"/> | Krishna | Testing first time | admin | 11 Mar, 2015 00:56:44 EDT | <input type="text" value="Select Action"/> |

The Custom Attribute Sets page displays the following:

- **New Custom Attribute Set:** Using this button, you can create a new custom attribute set.
- **Custom Attribute Set:** You can enter the name of the Custom Attribute Set.
- **Description:** This feature displays a description about the custom attribute set.
- **Last Modified by:** This feature displays the user who last modified the custom attribute set.
- **Last Modified on:** This feature displays the last modified date of the custom attribute set.
- **Actions:** You can select any action for a custom attribute set from the list of available options.
 - **Copy Custom Attribute:** Copy a custom attribute set. You cannot have the same name for the copied custom attribute set.
- **Delete:** Delete files.
- **Previous:** Clicking this button takes you to the previous page (if it exists).
- **Next:** Clicking this button takes you to the next page (if it exists).

You can do the following in the Custom Attribute Sets page.

- [Create a custom attribute set.](#)
- [Edit an existing custom attribute set.](#)
- [Delete an existing custom attribute set.](#)

6.6.1 How to Create a Custom Attribute Set

To create a custom attribute set, follow these steps:

1. In EMM management console, from **Settings**, click **Custom Attribute Sets**. The Custom Attribute Sets page appears.
2. Click **New Custom Attribute Set**. The New Custom Attribute Set dialog appears.
3. Enter a name in the **Custom Attribute Set Name** field.
4. Enter a description for the custom attribute in the **Description** field.
5. Click **Save** to create the custom attribute set, or click **Save & Edit** to create the custom attribute set and edit it.

6.6.2 How to Edit a Custom Attribute Set

To edit a custom attribute set, follow these steps:

1. In EMM management console, from **Settings**, click **Custom Attribute Sets**. The Custom Attribute Sets page appears displaying existing custom attribute sets.
2. Click the custom attribute set you want to edit. The Custom Attribute Set Details page appears.
3. Modify the details of the custom attribute set.
4. Click **Save & Exit** to save the changes you have made, and go to the Custom Attribute Sets page, or click **Save & Edit** to stay on the same page.

6.6.3 How to Delete a Custom Attribute Set

To delete a custom attribute set, follow these steps:

1. In EMM management console, from **Settings**, click **Custom Attribute Sets**. The Custom Attribute Sets page appears displaying existing custom attribute sets.
2. Click the custom attribute set you want to delete. A warning message appears asking you to confirm the delete.
3. Click **Yes**. A delete success message appears.
4. Click **OK**. The Custom Attribute Sets page appears.

6.6.4 Custom Attribute Set Details

The Custom attribute set detail page displays the following sections and fields.

Custom Attribute Set Details

[Custom Attribute Sets](#) > [Star Fleet](#)

Custom Attribute Set Details

Custom Attribute Set Name*

Description

| <input type="checkbox"/> | Attributes | Values | + Add Attribute |
|--------------------------|------------|--------|---------------------------------|
| No entries | | | |

[Delete](#)

[Save & Exit](#) [Save & Continue](#) [Cancel](#)

- **Custom Attribute Set Details:**
 - **Custom Attribute Set Name:** Displays the Custom Attribute Set name.
 - **Description:** Displays description about the custom attribute set.
- **Attributes:** Displays an attribute name.
- **Values:** Displays an attribute's associated value details.
- **Add Attribute:** Using this button, you can add an attribute.
- **Delete:** Delete files.
- **Save & Exit:** This feature allows you to save modifications you made on the Custom Attribute Set Details page and exit to the Custom Attribute Sets page.
- **Save & Continue:** This feature allows you to save modifications you made on the Custom Attribute Set Details page and remain on the same page.
- **Cancel:** The Cancel button allows you to cancel all changes you made in the Custom Attribute Set Details page.

6.6.5 How to Add an Attribute To a Custom Attribute Set

To add an attribute to an existing custom attribute set, follow these steps:

1. In EMM management console, from **Settings**, click **Custom Attribute Sets**. The Custom Attribute Sets page appears displaying existing custom attribute sets.
2. Click the custom attribute set, you want to add an attribute to. The Custom Attribute Set Details page appears.
3. Click **Add Attribute**. A new row is added below.
4. Enter the name in the **Attribute** field.
5. Enter the corresponding value for the attribute in the **Values** field.

6. Click **Save & Exit** to save the changes, and go to the Custom Attribute Sets page, or click **Save & Edit** to stay on the same page.

6.6.6 How to Delete an Attribute From a Custom Attribute Set

To delete an attribute from an existing custom attribute set, follow these steps:

1. In EMM management console, from **Settings**, click **Custom Attribute Sets**. The Custom Attribute Sets page appears displaying existing custom attribute sets.
2. Click the custom attribute set you want to delete an attribute from. The Custom Attribute Set Details page appears.
3. Select the attribute you want to delete using the selection button. The Delete button is enabled.
4. Click **Delete**. The attribute is deleted.
5. Click **Save & Exit** to save the changes, and go to the Custom Attribute Sets page, or click **Save & Edit** to stay on the same page.

6.6.7 Applying a Custom Attribute Set to a User

To apply a custom attribute set to a user, follow these steps:

1. In EMM management console, from **Access Management**, click **Users**. The Users page appears displaying existing users.
2. Click on the user you want to apply the custom attribute set to. The user details page appears.
3. In the User Details section, from **Custom Attributes** list, select the custom attribute you want to apply to the user.
4. Click **Save**. A success message appears.
5. Click **OK**. The Users page appears.

6.6.8 Applying a Custom Attribute Set to a Group

To apply a custom attribute set to a group, follow these steps:

1. In EMM management console, from **Access Management**, click **Groups**. The Groups page appears displaying existing groups.
2. Click on the group you want to apply the custom attribute set to. The Group details page appears.
3. In the Group Details section, from **Custom Attributes** list, select the custom attribute you want to apply to the group.
4. Click **Save**. A success message appears.
5. Click **OK**. The Groups page appears.

6.6.9 Applying a Custom Attribute Set to a Device

To apply a custom attribute set to a device, follow these steps:

1. In EMM management console, from **Device Management**, click **Devices**. The Devices page appears displaying existing devices.
2. Click on the device you want to apply the custom attribute set to. The Device details page appears.
3. Click **Asset Properties** tab. The Asset properties details appear.
4. From **Custom Attributes** list, select the custom attribute you want to apply to the device.
5. Click **Save & Exit**. A success message appears.
6. Click **OK**. The Devices page appears.

6.6.10 Applying a Custom Attribute Set to an App

To apply a custom attribute set to an App, follow these steps:

1. In EMM management console, from **App Management**, click **Enterprise Apps** or **VPP Apps**. The Enterprise Apps or VPP Apps page appears displaying existing apps.
2. Click on the app you want to apply the custom attribute set to. The App details page appears.
3. Click on the platform type tab - for example, Android or iPhone. The Platform tab details appear.
4. From **Custom Attribute Configuration** list, select the custom attribute you want to apply to the app.
5. Click **Save & Exit**. A success message appears.
6. Click **OK**. The Enterprise Apps or VPP Apps page appears.

6.7 Branding

There are several locations where Kony EMM app provides default branding. An administrator can add custom logos for branding. Branding can be changed on the Kony Management Web Console and enterprise store.

This section allows you to provide branding across EMM.

The maximum dimensions for your logos for each of the supported devices are specified. You can specify dimensions for your logos to maintain aspect ratio.

Note: If no settings are done to the Branding, the system uses the Kony icons for branding.

From the **Settings** section, click **Branding** from the left panel. The Branding page has two tabs:

- [Web Branding](#)
- [Enterprise Store Branding](#).

6.7.1 Web Branding

The Branding page appears with the default tab set as Web branding. The default tab has a list of icons used for branding the application.

The Web Branding page contains the following tabs:

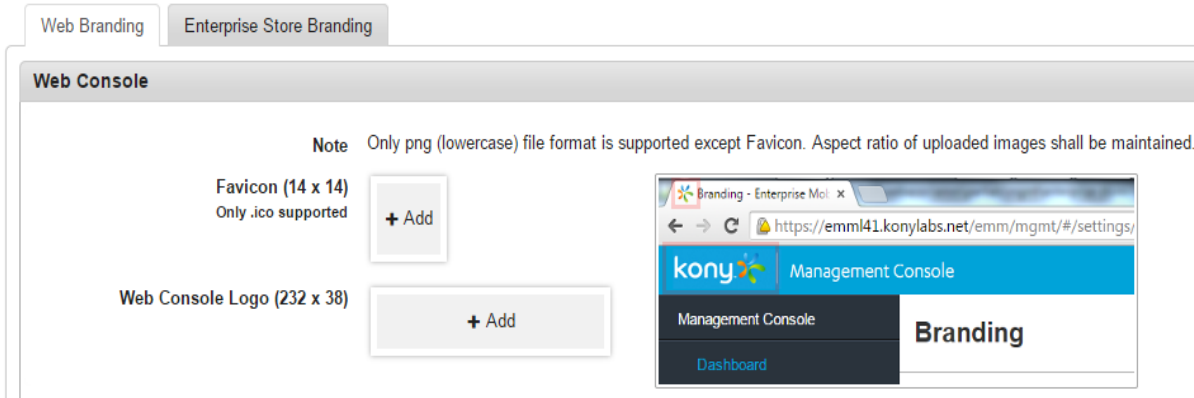
- [Web Console](#)
- [Enterprise Store Download Page](#)

The Enterprise Store Branding page contains **General** and **Branding Sets** sections.

6.7.1.1 Web Console

You can customize two images under web consoles. This applies to both Management Console and Self-Service Consoles.

Note: Only .PNG images are accepted for the Web Console logo and .ICO files for Favicon. The file is in proper format if %PNG exists in first line. Open the new file in notepad or notepad++, to check for %PNG in first line or header of file.



The Web Console page displays the following icons.

| Icons | Description |
|-----------------------------|---|
| Web Console Logo (232 x 38) | The application icon is the visual representation, at top left corner, of your app. Make sure that your application icon is clearly visible on any type of background. Dimensions of the application logo are as follows: <ul style="list-style-type: none"> • Size: 232 x 39 pixels • Color Mode: RGB, flattened, no transparency • File Type: High-quality PNG image file |

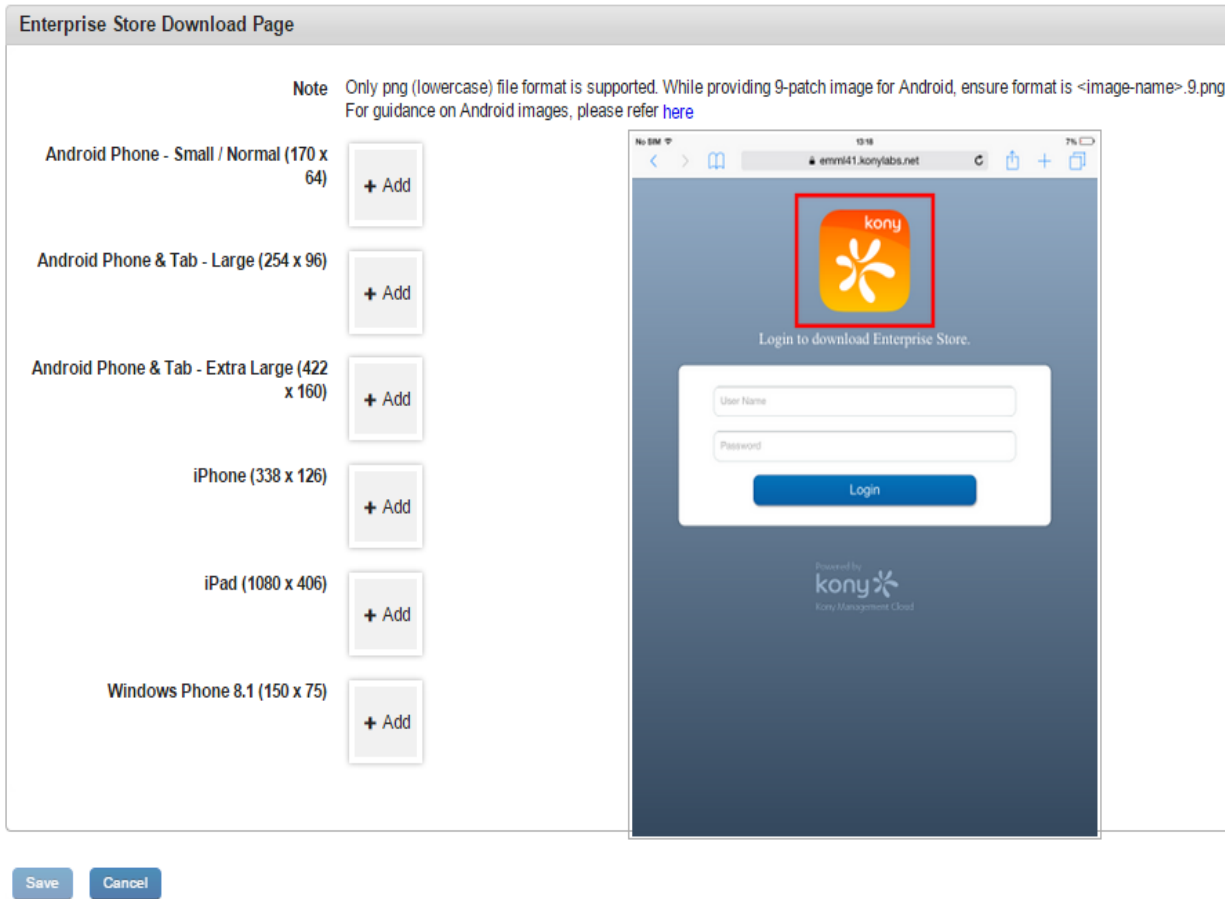
| Icons | Description |
|---------------------------------------|---|
| Favicon (14 x 14) Only .ico supported | <p>A favicon (short for favorites icon), is a shortcut icon, or bookmark icon. On the browser tab when EMM is open.</p> <p>Dimensions of the favicon are:</p> <ul style="list-style-type: none">• Size: 14 X14 pixels• Color Mode: RGB, flattened, no transparency• File Type: High-quality |

6.7.1.2 Enterprise Store Download Page

The Enterprise Store Download page that every device user must visit from the device to register devices.

The Enterprise Store Download Page icon size varies according to the supported device.

Note: Only PNG file format is supported. For guidance on Android images, please click [here](#).



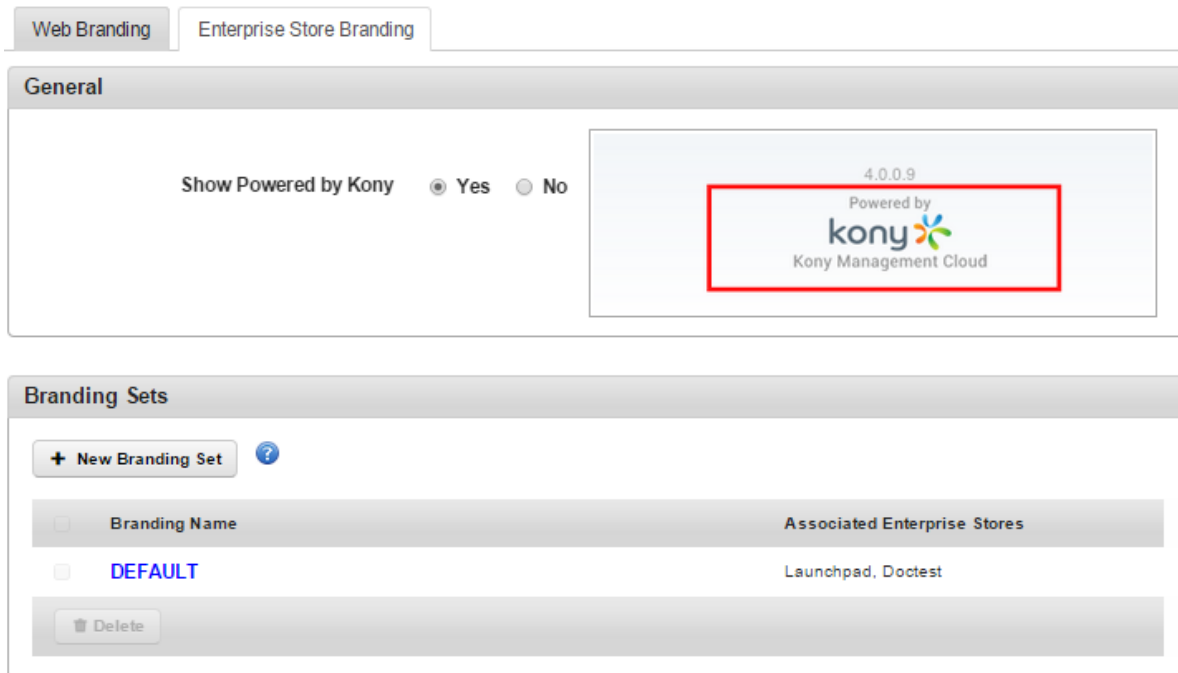
The Enterprise Store Download Page displays the following icon sizes for supported devices.

| Icons | Description |
|----------------------------------|--|
| Android Phone - Small and Normal | Dimensions of the log are: <ul style="list-style-type: none"> • Size: 170 x 64 pixels • File Type: High-quality PNG image file |
| Android Phone - Large | Dimensions of the logo are: <ul style="list-style-type: none"> • Size: 254 x 96 pixels • File Type: High-quality |

| Icons | Description |
|-------------------------------------|--|
| Android Phone and Tab - Extra Large | Dimensions of the logo are: <ul style="list-style-type: none">• Size: : 422 x 160 pixels• File Type: High-quality |
| iPhone | Dimensions of the logo are: <ul style="list-style-type: none">• Size: 338 x 126 pixels• File Type: High-quality PNG image file |
| iPad | Dimensions of the logo are: <ul style="list-style-type: none">• Size: 1080 x 406 pixels• File Type: High-quality PNG image file |
| Windows Phone 8.1 | Dimensions of the logo are: <ul style="list-style-type: none">• Size: 150 x 75 pixels• File Type: High-quality PNG image file |

6.7.2 Enterprise Store Branding

The Enterprise Store Branding page has two sections, **General** and **Branding Sets**.



In the **General** section, a Show Powered by Kony option is available.

- **Show Powered by Kony:** Options are **Yes** and **No**.
 - **Yes:** If configured to yes, the image **Powered by Kony** will appear on the enterprise store login screen and also on the enterprise store Download page.
 - **No:** If configured to No, the image **Powered by Kony** will not appear on the enterprise store login screen and also on the enterprise store Download page.

Ensure that the Enterprise store name you provide (in the Branding section) does not contain # sign in it. If the Enterprise store name has a # sign in it, downloading the enterprise store on the Samsung native browser **Internet** will fail.

The **Branding Sets** section displays a button and a table.

- **Add New Branding Set:** You can create a new branding set using this button.
- **Branding Sets table:** This table displays available branding sets. This table shows two columns.
 - **Branding Name:** Displays the name of the branding set.
 - **Associated Enterprise Stores:** Displays enterprise stores associated with the branding

set.

- **Delete:** You can delete a branding set by using this button.

You can do the following in the Enterprise Store Branding tab:

- [Create a New Branding Set](#)
- [Delete an Existing Branding Set](#)

6.7.2.1 Creating a New Branding Set

A branding set helps you to create a set for branding, that you can apply on an enterprise store.

To create a new branding set, follow these steps:

1. In the Kony Management Suite Management console, click **Branding**. The Branding page appears.
2. On the **Enterprise Store Branding** tab.
3. Click on **Add New Branding Set**. The Create New Branding Set page appears.
4. In the **Name** field, enter a name for the branding set you want to create.
5. Click **Create**. A Success page appears.
6. Click **OK**. The new branding set is created and appears in the branding sets table.

6.7.2.2 Deleting a Branding Set

To delete an existing branding set, follow these steps:

1. In Kony Management Suite Management console, click **Branding**. The Branding page appears.
2. Click **Enterprise Store Branding** tab. The Enterprise Store Branding tab details appear.
3. Select the branding set you want to delete, and click **Delete**. A Confirm Branding Deletion page appears.

4. Click **Yes**. A Success page appears.
5. Click **OK**. The branding set is deleted.

6.7.3 Branding Set

When you create a new branding set, all images and icons are configured by default. To change the icons and images, click on the branding set name, and edit all icons and images as required.

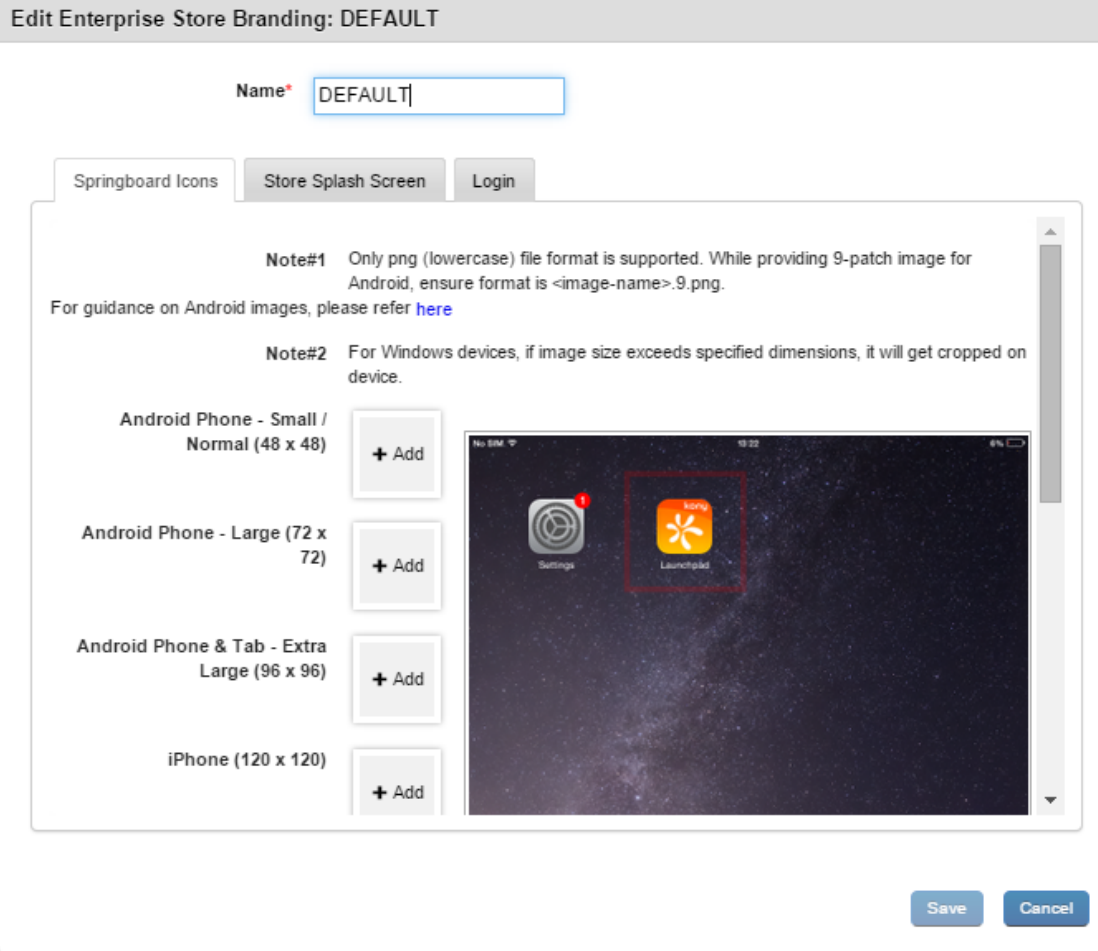
A branding Set page contains the following tabs:

- [Springboard Icons](#)
- [Store Splash Screen](#)
- [Login](#)

6.7.3.1 Springboard Icons

On the device's Springboard, the enterprise store icon is shown. An administrator can configure this icon as well to match with your application. The Springboard icon size varies according to the supported devices.

Note: Only PNG file format is supported. For guidance on Android images, please click [here](#).



The Springboard Page displays the following icon sizes for supported devices.

| Icons | Description |
|----------------------------------|--|
| Android Phone - Small and Normal | Dimensions of the logo are: <ul style="list-style-type: none"> • Size: 48 x 48 pixels • File Type: High-quality PNG image file |
| Android Phone - Large | Dimensions of the logo are: <ul style="list-style-type: none"> • Size: 72 x 72 pixels • File Type: High-quality PNG image file |

| Icons | Description |
|-------------------------------------|--|
| Android Phone and Tab - Extra Large | Dimensions of the logo are: <ul style="list-style-type: none"> • Size: 96 x 96 pixels • File Type: High-quality PNG image file |
| iPhone | Dimensions of the logo are: <ul style="list-style-type: none"> • Size: 120 x 120 pixels • File Type: High-quality PNG image file |
| iPad | Dimensions of the logo are: <ul style="list-style-type: none"> • Size: 152 x 152 pixels • File Type: High-quality PNG image file |
| Windows Phone 8.1 | Dimensions of the logo are: <ul style="list-style-type: none"> • Size: 62 x 62 pixels • File Type: High-quality PNG image file |
| Windows Phone 8.1 Small Tile | Dimensions of the logo are: <ul style="list-style-type: none"> • Size: 159 x 159 pixels • File Type: High-quality PNG image file |
| Windows Phone 8.1 Medium Tile | Dimensions of the logo are: <ul style="list-style-type: none"> • Size: 336 x 336 pixels • File Type: High-quality PNG image file |
| Windows Phone 8.1 Wide Tile | Dimensions of the logo are: <ul style="list-style-type: none"> • Size: 691 x 336 pixels • File Type: High-quality PNG image file |

6.7.3.2 Splash Screen

When the Enterprise store app is launched, a user sees a splash screen. An administrator can customize the image.

Note: Only the PNG file format is supported. While providing a 9 Patch image, ensure the format is .9.png.

For guidance on Android images, please click [here](#).

Springboard Icons Store Splash Screen Login

Note #1: Only png (lowercase) file format is supported. While providing 9-patch image for Android, ensure format is <image-name>.9.png.
For guidance on Android images, please refer [here](#)

Note #2: For Windows devices, only JPG format is supported.

Android Phone - Small / Normal (322 x 482) + Add

Android Phone - Large (539 x 856) + Add

Android Phone & Tab - Extra Large (807 x 1282) + Add

iPhone (640 x 960) + Add

Save Cancel

The Enterprise Store Splash Screen displays the following icon sizes for supported devices.

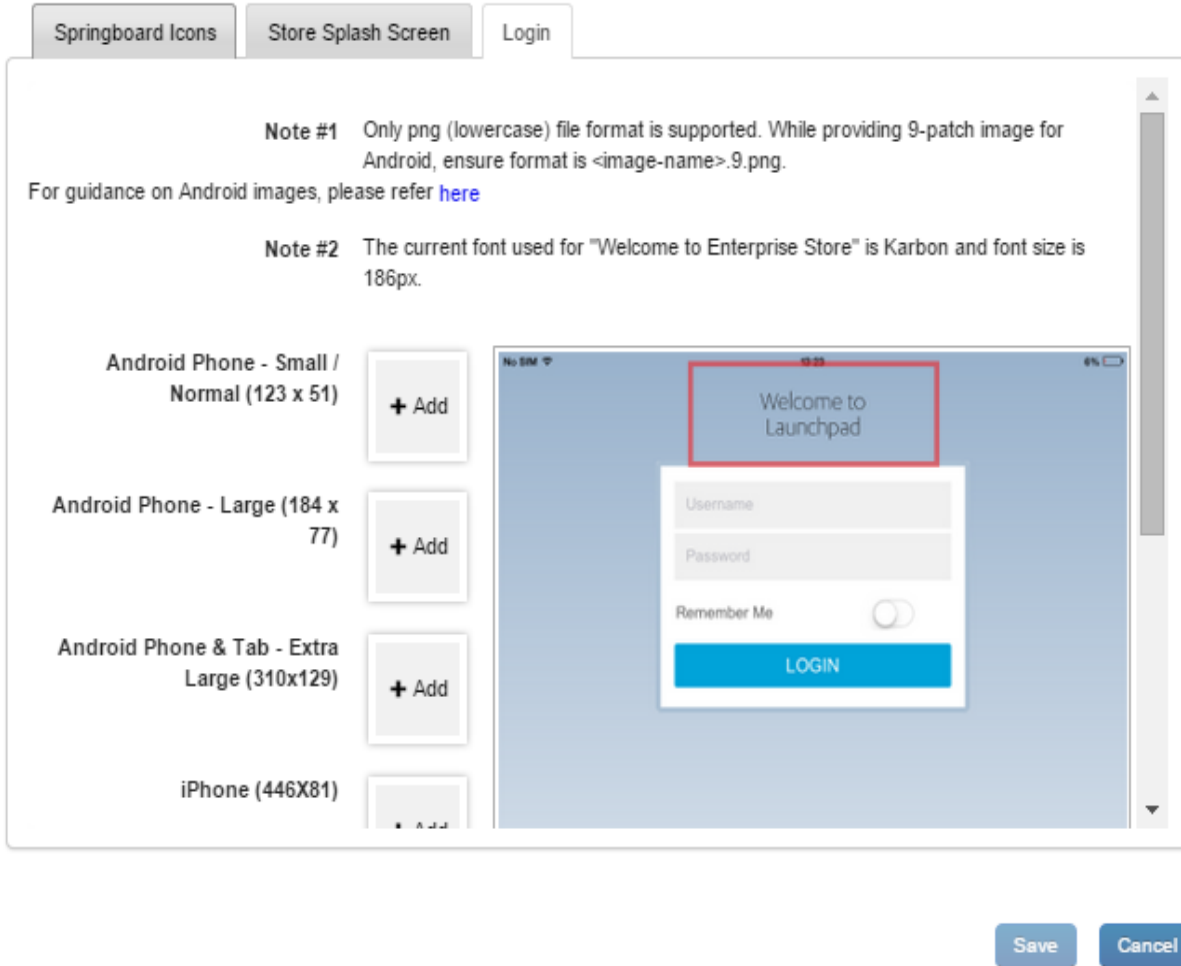
| Icons | Description |
|-------------------------------------|---|
| Android Phone - Small and Normal | Dimensions of the logo are: <ul style="list-style-type: none"> • Size: 322 x 482 pixels • File Type: High-quality PNG image file |
| Android Phone - Large | Dimensions of the logo are: <ul style="list-style-type: none"> • Size: 539 x 856 pixels • File Type: High-quality PNG image file |
| Android Phone and Tab - Extra Large | Dimensions of the logo are: <ul style="list-style-type: none"> • Size: 807 x 1282 pixels • File Type: High-quality PNG image file |
| iPhone | Dimensions of the logo are: <ul style="list-style-type: none"> • Size: 640 x 960 pixels • File Type: High-quality PNG image file |
| iPhone 5 | Dimensions of the logo are: <ul style="list-style-type: none"> • Size: 640 x 1136 pixels • File Type: High-quality PNG image file |
| iPhone 6 (Portrait) | Dimensions of the logo are: <ul style="list-style-type: none"> • Size: 750 x 1334 pixels • File Type: High-quality PNG image file |
| iPhone 6 (Landscape) | Dimensions of the logo are: <ul style="list-style-type: none"> • Size: 1334 x 750 pixels • File Type: High-quality PNG image file |

| Icons | Description |
|---------------------------|---|
| iPhone 6 Plus (Portrait) | Dimensions of the logo are: <ul style="list-style-type: none"> • Size: 1242 x 2208 pixels • File Type: High-quality PNG image file |
| iPhone 6 Plus (Landscape) | Dimensions of the logo are: <ul style="list-style-type: none"> • Size: 2208 x 1242 pixels • File Type: High-quality PNG image file |
| iPad | Dimensions of the iPad touch icon are: <ul style="list-style-type: none"> • Size: 1536 x 2048 pixels • File Type: High-quality PNG image file |
| Windows Phone 8.1 WVGA | Dimensions of the iPad touch icon are: <ul style="list-style-type: none"> • Size: 480 x 800 pixels • File Type: JPG image file |
| Windows Phone 8.1 WVGA | Dimensions of the iPad touch icon are: <ul style="list-style-type: none"> • Size: 768 x 1280 pixels • File Type: JPG image file |
| Windows Phone 8.1 720p | Dimensions of the iPad touch icon are: <ul style="list-style-type: none"> • Size: 720 x 1280 pixels • File Type: JPG image file |

6.7.3.3 Login Screen

Once the enterprise store app is launched, a user lands on the login page and must provide credentials to use the app. An administrator can customize the icon on the page.

Note: Only the PNG file format is supported. For guidance on Android images, please click [here](#).



The enterprise store app Login Screen displays the following icon sizes for supported devices.

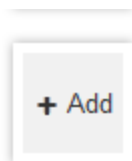
| Icons | Description |
|----------------------------------|---|
| Android Phone - Small and Normal | Dimensions of the logo are: <ul style="list-style-type: none"> • Size: 123 x 51 pixels • File Type: High-quality PNG image file |

| Icons | Description |
|-------------------------------------|--|
| Android Phone - Large | Dimensions of the logo are: <ul style="list-style-type: none"> • Size: 184 x 77 pixels • File Type: High-quality PNG image file |
| Android Phone and Tab - Extra Large | Dimensions of the logo are: <ul style="list-style-type: none"> • Size: 310 x 129 pixels • File Type: High-quality PNG image file |
| iPhone | Dimensions of the logo are: <ul style="list-style-type: none"> • Size: 446 x 81 pixels • File Type: High-quality PNG image file |
| iPad | Dimensions of the logo are: <ul style="list-style-type: none"> • Size: 800 x 140 pixels • File Type: High-quality PNG image file |
| Windows Phone 8.1 | Dimensions of the logo are: <ul style="list-style-type: none"> • Size: 456 x 166 pixels • File Type: High-quality PNG image file |

6.7.4 Uploading logos

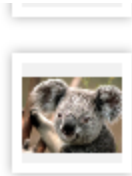
To upload your logos for Branding, follow these steps:

Android (401x73)



1. To upload an icon, click the **+Add** button to select the icon from its location.

Android (401x73)



2. Select the icon, and click Open. The icon appears for the selected device agent.

Android (401x73)



3. To remove the existing icon, place the pointer at the right corner of the image and click the delete (**X**) icon. This action removes the existing icon.
4. Click the **Save** button to save the icon. In the confirmation message that appears, click **OK** to return to the main page.

6.8 Geo and Time Fence List

This is a master list of all the Geo-fences and Time fences that can be used on MDM or MAM. Based on requirement, you can create multiple Geo-fences and Time fences.

From the **Settings** section, click **Geo and Time Fence List** from the left panel. The Geo and Time Fence List Page include two tabs: Geo-fence and Time Fence. The Geo and Time Fence List page appears with a list of all the Geo-Fences along with their Descriptions. You can search the Geo-Fence based on each column and also sort on each column.

Important: On Android devices, the Geo fence policy does not work as expected. This is a known issue.

Important: When you alter a Geo fence, a trigger is not sent to enrolled devices to update their device settings.

| Geo-fence Name | Description | Created By | Last Modified On |
|--|---|--|----------------------------------|
| <input type="text" value="Search Geo-fence Name"/> | <input type="text" value="Search Description"/> | <input type="text" value="Search Created By"/> | <input type="text" value="All"/> |
| <input type="checkbox"/> kony | | admin | 06 Oct, 2013 22:57:24 MHT |
| <input type="checkbox"/> Texas | | admin | 06 Oct, 2013 22:56:17 MHT |

Geo- fence List view displays the following columns:

| Properties | Description |
|----------------|---|
| Geo-fence Name | Displays the name of the Geo-fence program. |

| Properties | Description |
|------------------|---|
| Description | Displays the brief description of the Geo-fence program. |
| Created By | Displays the owner name. |
| Last Modified On | Displays the date on which the Geo-fence was last modified. |

You can perform the following activities from this page:

- [Searching a Geo-fence](#)
- [Creating a Geo-fence](#)
- [Deleting a Geo-fence](#)
- [Searching a Time Fence](#)
- [Creating a Time fence](#)
- [Deleting a Time Fence](#)

6.8.1 Searching a Geo-fence

You can search a Geo-fence through search filters based on all the grid columns. You can apply a single or a combination of search filters to define the search criteria and get the refined outcome.

To search a Geo-fence, follow these steps:

1. **Geo Fence Name:** Enter partial or complete name in the **Search Geo Fence Name** field.
2. **Description:** Enter the specific details in the **Search Description** field.
3. **Created By:** Enter partial or complete name of the Administrator in the **Search Created By** field.
4. **Last Modified On:** Select the required option from the drop-down list.

5. According to your search filter criteria, the list view is updated with respective Geo-fence details. By default, the list view displays ten Geo-fences according to Display settings, which you can modify through Display drop-down list. You can also scroll through the list view through Previous and the Next button.

6.8.2 Creating a Geo-fence

To create a new Geo-fence program, follow these steps:

Geo & Time Fences

+ New Fence

1. On the Geo & Time Fence List screen, click the + **New Fence** button.

New Fence x

Choose Fence Type Geo-fence Time Fence

Geo-fence Name*

Description

Create & Edit Cancel

2. The **New Fence** window appears. Enter the following details:
 - a. **Choose Fence Type:** By default, this option is set to **Geo-fence** that you can modify to Time Fence.
 - b. **Geo Fence Name:** Enter a valid name for the Geo-fence. This action enables the **Create and Edit** button.

- c. **Description:** Enter a brief description of the Geofence. The description should accurately describe the features and functionality of Geo-Fence.

3. Click the **Create & Edit** button.

Geo-fence details page appears.

4. Enter details for the following fields:

The screenshot displays the configuration interface for a Geo-fence. On the left, there is a form with the following fields:

- Geo-fence Name:** Guatemala Nation
- Location Set:** 5, San Antonio Las Cuevas, Guatemala (with a search icon and a note: "or drag red pin to location")
- Radius Area:** 200 miles (with a note: "or drag blue pin to resize radius")
- Description:** Geofence Policy (with a character count: "You have 484 characters left" and a "Reset" button)

On the right, a map of Central America is shown with a red pin on Guatemala and a blue circle representing the 200-mile radius. The map includes labels for various countries and cities, such as Mexico, Guatemala, Belize, Honduras, Nicaragua, Costa Rica, Panama, Colombia, and Ecuador.

- a. **Geo-fence Name:** Displays geo-fence name.
- b. **Location Set:** Drag the red icon on map. Based on location position and entered radius area, location set details appear for example, 5, San Antonio, Las Cuevas, Guatemala.

The larger Geofence takes precedence. In the image displayed above, the bigger radius Geofence **Guatemala Nation** (200 miles) takes precedence over smaller radius Geofence **Guatemala City** (10 miles) when the device is kept in Guatemala City.

For example, a device named **ABC** is part of two device sets **DS1** and **DS2**.

On **DS1**, Passcode policy No. 1 is applied with **Guatemala Nation** (Allow).

On **DS2** Passcode policy No. 2 is applied with **Guatemala City (Allow)**.

When the device is kept in Guatemala City, Passcode policy No. 1 is applied because the Geofence attached to **Policy No 1** is larger and completely encompasses the Geofence applied to policy no. 2.

- c. **Description:** This field is pre-populated with the existing details. If required, you can update this field.

5. Click the **Save** button. In the success message that appears, click OK to return to the main page.

Important: Allow GPS Location Monitoring: Deny policy is not working for [Android OS 4.1.1](#).

6.8.3 Deleting a Geo-fence

If a Geo-fence is no longer applicable to a device, you can delete it.

| | | | | |
|-------------------------------------|--------------|----------------------|--------------------------------------|----------------------------|
| <input checked="" type="checkbox"/> | Hyderabad | Testing Geo Policyff | akram ali | 12/28/2013 10:45:02 AM EST |
| <input type="checkbox"/> | Hyderabad123 | Hyderabad123 | sridharreddy123SridharReddy123S r | 12/28/2013 09:53:35 AM EST |
| <input type="checkbox"/> | Anupam | | akram ali | 12/28/2013 09:01:56 AM EST |

To delete a Geo-fence, follow these steps:

1. Select the required Geo-fence through the check box next to it in the list view.
2. Click the **Delete** button.
3. In the warning message (Delete Geo-fences) that appears, click Yes to continue.
4. In the success message that appears, click OK to return to the main page.

The deleted Geo-fence is no longer displayed in the list view.

6.8.3.1 Geo-fence Functionality for Windows Phone 8.x

The Geofence functionality for the Windows Phone 8.x is as follows:

Scenario 1

If a Geo-fence is already created before the registration of a device, then after registering the device, Geo-fence becomes effective immediately.

Scenario 2

If a Geo-fence is created or modified after a device is registered, then unlike iOS and Android it does not reflect immediately.

It takes x amount of time, before it starts reflecting. This x amount is configurable at design time.

The Windows Phone 8 device has a heartbeat from the container app (Kony) and a sync interval from the inbuilt device app. In heartbeat, admin gives the location details to the service. In sync interval, the device app pulls in any new policies/commands and applies them.

The heartbeat when the app is in foreground is 15 minutes and when the app is in back ground is 30 minutes. The Sync interval can be set by the admin in device settings and has a minimum value of 30 minutes.

Since in every heartbeat, admin brings any new/modified Geo-fences (which is 30 minutes or less), the policies based on the Geo-fence certainly comes to the device that happens in every Sync Interval (it is a minimum of 30 minutes).

To summarize, if the admin modifies or creates a new Geofence, it is applied in the next immediate sync that is 60 minutes, by default.

6.8.4 Searching a Time Fence

You can search a Time Fence through the search filters based on all the grid columns. You can apply a single or a combination of search filters to define the search criteria and get the refined outcome.

To search a Time Fence, follow these steps:

1. **Time Fence Name:** Enter partial or complete name in the **Search Time Fence Name** field.
2. **Description:** Enter the specific details in the **Search Description** field.
3. **Created By:** Enter partial or complete name of the Administrator in the **Search Created By** field.
4. **Last Modified On:** Select the required option from the drop-down list.
5. According to your search filter criteria, the list view is updated with respective Time Fence details. By default, the list view displays ten Time Fences according to Display settings, which you can modify through Display drop-down list. You can also scroll through the list view through Previous and the Next button.

6.8.5 Creating a Timefence

Time fences are created to indicate a duration of time during which certain activities must or must not be done. They are typically used with device and app policies.

From the **Settings** section, click **Geo and Time Fence List** from the left panel. The Geo and Time Fence List page appears with a list of the Geo-Fence(s) details. Click the Time Fence tab to open Time Fence page. The list view displays a list of all the Time Fences along with their description. You can search the Time Fences based on each column.

Geo & Time Fences

[+ New Fence](#)

Geo-fence
Time Fence

Displaying 1 - 1 of 1 - Display 10

| | Time Fence Name | Description | Created By | Last Modified On |
|--------------------------|---|---|--|----------------------------------|
| | <input type="text" value="Search Time Fence Name"/> | <input type="text" value="Search Description"/> | <input type="text" value="Search Created By"/> | <input type="text" value="All"/> |
| <input type="checkbox"/> | Aktiv | | Kony EMM | 08 Nov, 2014 20:40:36 IST |

[Delete](#)
[Previous](#) **Page (1/1)** [Next](#)

Time Fence(s) List view displays the following columns:

| Properties | Description |
|------------------|--|
| Time Fence Name | Displays the name of the Time Fence program |
| Description | Displays the brief description of the Time Fence program. |
| Created By | Displays the owner name. |
| Last Modified On | Displays the date on which the Time Fence was last modified. |

To create a new Time Fence program, follow these steps:

Geo & Time Fences

[+ New Fence](#)

1. To open the New Fence window, click the **+ New Fence** button next to the Geo and Time Fence List label at the top of the page.

New Fence
x

Choose Fence Type Geo-fence **Time Fence**

Time Fence Name*

Description

For Nevada state|

You have 484 characters left

New Fence window appears.

2. Enter the following details:

a. **Choose Fence Type:** By default, this option is set to Timefence, which you can modify to Geofence.

b. **Timefence(s) Name:** Enter a valid name for the Timefence.

This action activates the **Create and Edit** button.

c. **Description:** Enter a brief description of the Timefence. The description should accurately describe the features and functionality of the Timefence.

3. Click the **Save and Edit** button to update the Time Fence immediately.

Time Fence Details
Time Fence List > Time Fence Details

Time Fence Basics

Time Fence Name* Nevaa State

Description For Nevada state

You have 484 characters left

Specify Time Fence

Days Mon Tue Wed Thu Fri Sat Sun

Hours From: HH:mm To: HH:mm

Save Cancel

The Time Fence details page appears.

4. Enter details for the following fields:

a. **Time Fence(s) Basics:**

- i. **Timefence(s) Name:** Displays timefence name.
- ii. **Description:** This field pre-populates with the existing details. If required, you can update the description.

b. **Specify Time Fence:**

- i. **Specify Days:** Select the weekday, when you wish to specify the time fence.
- ii. **Specify Business Hours:** If you select the Yes option, **From** and **To** fields becomes active.

Specify Time Fence(s)

Restrict Usage on Certain Days Yes

Specify Days to Restrict Morning

Restrict App Usage to Business Hours Yes

Specify Business Hours From: 04:00 To: HH:mm (GMT+5:30) Bomba

Choose Time

Time 04:00

Hour

Minute

Now Done

- iii. Click your cursor in the **From** field to open the **Choose Time** window. Use the slider to select the time in hours and minutes. Click the **Done** button to close the window.

Click the cursor in the **To** field to open the **Choose Time** window. Use the slider to select the time in hours and minutes. To set the current time, click the **Now** button. Click the **Done** button to close the window.

A timefence is created from a range of hours specified at the **From** and **To** fields. A timefence is applied only if at least a day is selected. If you have not selected a day for a timefence, the system does not allow you to save a timefence. A timefence always starts from your server time.

Example 1:

If a timefence is set for 8 p.m to 8 a.m for Monday, then the total number of hours in the timefence range splits into two parts for Monday as follows:

Monday - 12.00 am to 08.00 am

Monday - 08.00 p.m to 12.00 a.m

Example 2:

If a timefence is set for 8 p.m to 8 a.m for Monday and Tuesday, then total number of hours in the timefence range splits into two parts for Monday and Tuesday as follows:

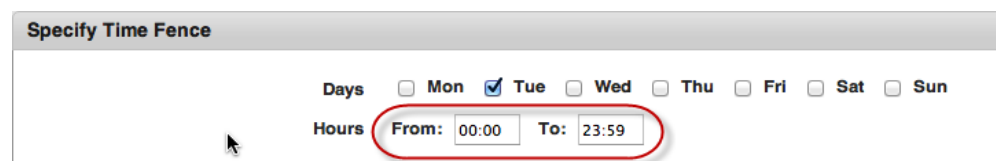
Monday - 12.00 a.m to 08.00 a.m

Monday - 08.00 p.m to 12.00 a.m

Tuesday - 12.00 a.m to 08.00 a.m

Tuesday - 08.00 p.m to 12.00 a.m

When the administrator changes the time zone settings on the portal, the server does not update or resolve the policies immediately. Policy resolution occurs when a device submits the heartbeat.



Specify Time Fence

Days Mon Tue Wed Thu Fri Sat Sun

Hours From: 00:00 To: 23:59

Note: The time zone applied for the timefence is derived from the value specified in the Device Settings.
Even though you have **From** > **To** fields in terms of time, the server logic respects the **To** value until 23:59 . If you enter values from 21:00 to 3:00, the server interprets values as 21:00 to 23:59 only

5. Click the **Save** button. In the success message that appears, click OK to return to the main page.

Click the **Cancel** button to close the window.

When Admin changes the time zone settings on the portal, only the time zone changes, but the values of time zone remain the same. The time fence values are not automatically adjusted as per the new time zone provided.

6.8.6 Deleting a Time Fence

If a Time Fence program is no longer applicable to a device, you can delete it.

To delete a Geo-fence, follow these steps:

1. Select the required Time Fence through the check box next to it in the list view.
2. Click the **Delete**.
3. In the warning message (Delete Time Fence) that appears, click **Yes** to continue.
4. In the success message that appears, click **OK** to return to the main page.

The deleted Time Fence is no longer displayed in the list view.

6.9 Language Settings

Kony Management 4.1 supports internationalization. Internationalization (i18N) is the ability of an application to show the content based on a locale, which is a combination of language and country, chosen in a user's device settings.

In Kony Management 4.1, the enterprise app store supports i18N. The feature allows end users to use their enterprise app store in their native language or their language of choice. Using the i18N feature, an administrator can upload translations for text that appears in the Kony enterprise store (Launchpad). Administrators can upload separate files for translations for all languages that they want to support.

An administrator can export data with all keys that are translated in the enterprise store app with the appropriate description and English translation. An administrator can add a translation for each key individually. For child apps deployed in Kony enterprise store, the default file is generated based on what a user provides as the app name and description from the app details page.

In Kony Management 4.1, internationalization is supported for the following features:

- Application store (except Kony Enterprise App Store names)
- App details
- Push messages
- Policy alert and error messages
- Terms and conditions

Important: On iOS and Windows devices, terms and conditions might still appear in English irrespective of the locale. After device enrollment, if a user logs out of the enterprise store, and if terms and conditions are modified, when the user logs into the store, terms and conditions appear in English.

The Language Settings page contains two tabs. Enterprise Store, and Enterprise Apps. By default, the Language Settings page opens in the Enterprise Store tab.

6.9.1 Enterprise Store Tab

The Enterprise Store tab displays the details of locales along with other details. On the Enterprise Store tab, you can create new locales, modify existing locales, delete a locale, and download an existing locale configuration.

Language Settings

| Locale Id | Locale Name | Locale Name (Native) | Created On | Last Updated On |
|-----------|-------------|----------------------|---------------------------|--|
| en | English | English | 02 May, 2016 15:42:34 IST | 02 May, 2016 15:42:41 IST Version 1 |

The Enterprise Store tab displays the following user interface features:

| Feature | Description |
|------------------|--|
| Add New Locale | You can create a new locale using this button. |
| Select Check Box | If selected at the row level, the particular locale is selected for further actions. Multiple rows can also be selected. Selection can only be done on a single page of records. You can choose to display up to 100 records (locales). |
| Locale ID | Displays the locale ID as provided by the administrator. The Locale ID is a combination of the language code along with the country code. The country code is optional. For example, for USA English, the locale ID is en_US. For British English, the ID is en_UK. For English as is, the language ID is en. The language ID is always lowercase while the country code is uppercase. |

| Feature | Description |
|----------------------|---|
| Locale Name | Displays the name of the locale as provided by the administrator. |
| Locale Name (Native) | Displays the name of the locale in the local language as provided by the administrator. |
| Created On | Displays the date and time when the locale is created. |
| Last Updated On | Displays the date and time when the locale is last modified. |
| Export | Downloads the current locale Excel file. |
| Delete | Using the delete button, you can delete selected locales. The button is active when the check box next to locale ID is selected, or if the multiselect check box is selected. |
| Previous | Clicking the button takes you to the previous page (if it exists). |
| Next | Clicking the button takes you to the next page (if it exists). |

6.9.2 Enterprise Apps Tab

The Enterprise Apps tab displays the details of existing enterprise apps in Kony Management server . On the Enterprise Apps tab, you can provide internationalization support to show app details of existing enterprise apps in the enterprise app store. For an existing enterprise app, you can add or modify the existing internationalization configuration.

Language Settings

Enterprise Store Enterprise Apps

Displaying 1 - 1 of 1 - Display 10 ▼

| App Name | Last Modified | |
|----------|---------------------------|---|
| App Name | | |
| app1 | 17 May, 2016 19:48:11 IST | <input type="button" value="↓"/> <input type="button" value="↑"/> |

Previous Page {1/1} Next

The Enterprise Apps tab contains the following user interface elements:

| Feature | Description |
|---------------|---|
| App Name | Displays the name of the app. |
| Last Modified | Displays the date and time when the app is last modified. |
| Export | Downloads the current app internationalization Excel (.xlsx) file. |
| Import | Uploads the app internationalization Excel (.xlsx and .xls) file to Kony Management server. |
| Previous | Clicking the button takes you to the previous page (if it exists). |
| Next | Clicking the button takes you to the next page (if it exists). |

6.10 Internationalization on Devices

A administrator creates a (on the Enterprise Store tab) is created in Kony Management server. If a device has a corresponding locale, when the user logs into the Kony Enterprise store (previously Launchpad), the locale is downloaded onto the device.

For example, the device's default language is French. When an **fr** locale is created in Kony Management administrator console through the Language Settings page, the locale will be downloaded on the device during the first log-in of the device after the locale is created.

In another example, a new locale (applicable) is created when the enterprise app is in the foreground. When the app goes to the background and returns to the foreground, a message appears that locale assets are being downloaded. Once the download is complete, the language on the enterprise app store will change according to the new locale.

Additionally, when a locale is modified and a user logs into the enterprise store, the updated locale data is downloaded onto the device. When a user is using the enterprise store, and the device's locale is modified, the user gets a message on the screen that the enterprise language is modified and is applied on the device.

In cases where the device language setting does not have a corresponding locale, English is displayed as the default locale and language. When a user is using the enterprise app store or a child app and the locale is deleted, the language will not change. The change will appear when the app goes to the background and returns to the foreground.

6.11 Working with Internationalization

In the Language settings page, you can do the following:

- [Create a new locale](#)
- [Modify an existing locale](#)
- [Delete an existing locale](#)


- [Work with the locale excel file](#)
- [Modify an existing Enterprise App locale](#)

6.11.1 How to Create A New Locale

To create a new locale, follow these steps:

1. In EMM management console, from **Settings**, click **Language Settings**. The Language Settings page appears. The Enterprise Store tab is open by default.
2. Click the **Add New Locale**. The New Locale page appears.


New Locale

Locale ID * 

Locale Name

Locale Name (Native)

Upload Locale File *

 Download Reference Configuration

3. Enter the following details:
 - a. **Locale ID:** Enter the locale ID. For example, for Spanish for Mexico, the locale ID is es_MX or, es for Spanish.

Important: The language ID appears can be in two formats:

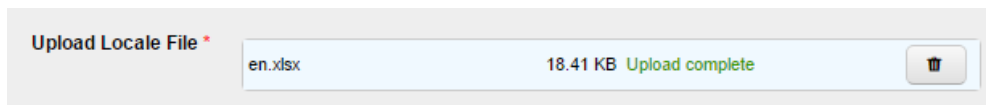
The Locale ID follows the format of <2 char language code>_<2 char country code>. For example, **es_MX**.

The Locale ID follows the format <two char language code>. For example, **es**.

If you do not give a locale ID in the standard format, the locale will not reflect on the device.

For more information on references, click [here](#).

- b. **Locale Name:** Enter the locale name. For example, Spanish.
 - c. **Locale Name (Native):** Enter the locale name in the native language. For example, Español -es_MX .
4. **Update Locale File:** To upload your locale file, click the **Add** button. File explorer opens.
 5. Navigate to the location of your locale file. For more information on how to work with a locale file, click [here](#).
 6. Select the file, and then click **Open**. The file is uploaded.



7. Click **Create**. A success message appears.
8. Click **OK**.

Your locale is now created and appears on the language settings page.

6.11.2 Modifying an Existing Locale

To modify an existing locale, follow these steps:

1. In the EMM management console, from **Settings**, click **Language Settings**. The Language Settings page appears. The Enterprise Store tab opens by default.
2. Click on the locale you want to modify. The Edit Locale page appears.

Edit Locale

Locale ID es_MX

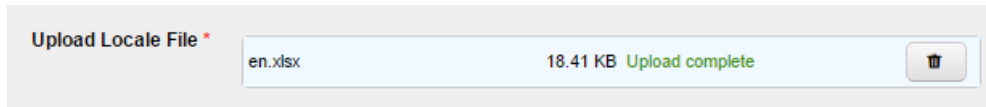
Locale Name

Locale Name (Native)

Update Locale File

3. You can modify the following fields:
 - a. **Locale Name:** You can modify the locale name. For example, from Spanish to Mexican Spanish.
 - b. **Locale Name (Native):** Enter the locale name in the native language. For example, Español Mexicano.
4. **Update Locale File:** You can upload a new locale file. To upload your new locale file, click the **Add** button. The file explorer opens.
5. Navigate to the location of your locale file.

6. Select the file, and then click **Open**. The file is uploaded.



7. Click **Create**. A success message appears.
8. Click **OK**.

Your locale is now modified, and modification details appear on the language settings page. Every time you upload a new locale file, the version of the locale file is modified by one version. For example, from Version 1 to Version 2.

6.11.3 How to Delete an Existing Locale

To delete an existing locale, follow these steps:

1. In the EMM management console, from **Settings**, click **Language Settings**. The Language Settings page appears. The Enterprise Store tab is open by default.
2. Select the locale you want to delete. The Delete button is enabled.
3. Click **Delete**. The Delete Locales message appears.
4. Click **Yes**. A success message appears.
5. Click **OK**.

Your locale is now deleted.

6.11.4 Working With the Locale Excel File

A locale file is an Excel file in a format where information entered can be read by the Kony Management server to display appropriate languages on a device when a locale is in force.

The Excel file contains the following tabs:

- Enterprise Store UI
- Enterprise Store messages
- Policy error messages
- Push message templates
- Terms and conditions

In each tab, you can provide translation in the language you want to support. Each tab contains four columns by default. Do not change anything from columns A to C.

To work with an existing locale, follow these steps:

1. In the EMM management console, from **Settings**, click **Language Settings**. The Language Settings page appears. The Enterprise Store tab is open by default.
By default, the English language locale (**en**) exists in the management console.
2. Click on the locale. The Edit Locale page appears.
3. Click Download Current Configuration. The locale file downloads to your system.
4. Open the locale Excel file in edit mode. The file opens.
Do not change anything from columns A to C.
5. In column D, rename the heading of the column to the language you want to support. For example, if you want to provide translations for French, replace **Text in Current: 'en'** with **Text in Current : 'fr'**.
6. For all rows, provide translation for column C in column D. For example, for row three, for **Access denied**, enter your translation in French as **Accès refusé**.
7. Once you are done with your translations, save and close the file.
It is recommended that the file name and your locale name be the same. For information on how to create a new locale, click [here](#).

Important: Ensure that you provide translation for at least one row in column D in the Excel file. Otherwise, the default text in column D will be considered as the translation. If you do not want to provide any translation, leave the fields blank.

6.11.5 Modifying an Existing Enterprise App Locale

When you upload an enterprise app to Kony Management, a locale (Excel file) is automatically created for the app to support internationalization. You can download the locale from the Export button in the Enterprise Apps name tab.

The Excel file will have the following sheets:

- App Data
- Android
- Android Table
- iPhone
- iPad
- Windows Phone 8.1+

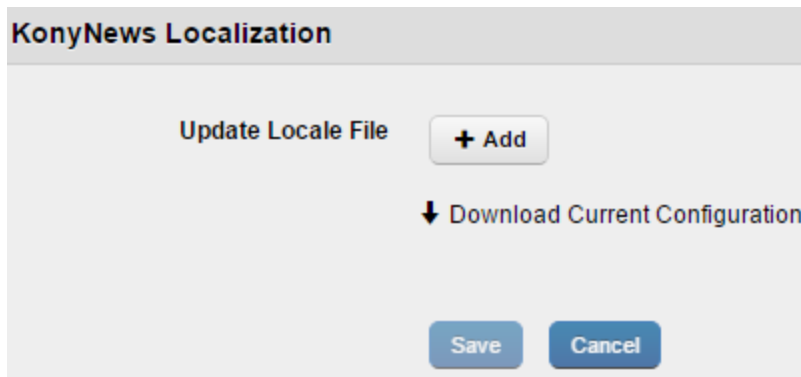
The sheets display four columns by default: **Version** (not available in the App Data sheet), **Key**, **Description** and **en**. Based on locales in the language settings page, additional columns will appear. For example, if the French locale is added in the language settings page, a new column **fr** will be added to the Excel file.

You can download (export) the Excel file to your system, provide required translations for any language in the Excel file's locale column and upload the file in the Enterprise Apps tab.

You can modify the internationalization for an app that you own. You cannot update an app that you do not own. This is applicable to various app versions as well.

To modify a locale for an enterprise app, follow these steps:

1. In the EMM management console, from **Settings**, click **Language Settings**. The Language Settings page appears. The Enterprise Store tab is open by default.
2. Click **Enterprise Apps** tab. The Enterprise Apps tab appears.
3. To update internationalization for the enterprise app, click **export**. An Excel file downloads to your system.
4. Open the Excel file, update the required translations, and save the file.
5. To upload the file to Kony Management console, click on the enterprise app's corresponding **import** button. The Localization page appears.



6. Click **Add**. The File explorer opens.
7. Navigate to the location of your locale file.
8. Select the file, and then click **Open**. The file is uploaded.
9. Click **Save**. A success message appears.
10. Click **OK**. Your enterprise app locale file is now updated. Every time you upload a new locale file, the previous version of the locale file is replaced by the new version.

Important: Do not modify the order of the columns in the Excel sheets.

6.12 Event Log

Event Log page displays a list of all the actions for a particular device, device set or policy that you or another user as admin initiated. For example, if you performed a Force Check-in, this action is displayed in the Event Log. Information from the event log can be helpful for troubleshooting.

From the **Settings** section, click the **Event Log** from the left panel. The Event Log page appears with a list of the logged events. The list view displays a list of all the actions along with other details. You can search the actions based on each column and also sort on each column.

Event Log

Displaying 1 - 10 of 37 - Display

| Action ▼ | Object Type | Object Name | Initiated By | Time Stamp |
|--|----------------------------------|---|--|---|
| <input type="text" value="Search Action"/> | <input type="text" value="All"/> | <input type="text" value="Search Object Name"/> | <input type="text" value="Search Initiated By"/> | <input type="text" value="Start Time"/> <input type="text" value="End Time"/> |
| Management Console Login | LOCAL | ramu v | Admin Activity | 07 Aug, 2017 05:32:10 EDT |
| Management Console Login | LOCAL | ramu v | Admin Activity | 07 Aug, 2017 03:50:45 EDT |
| Device enrolled | Device | admin | Device Initiated Enrollment | 07 Aug, 2017 03:40:15 EDT |
| Management Console Login | LOCAL | ramu v | Admin Activity | 07 Aug, 2017 03:29:13 EDT |
| Management Console Login | LOCAL | ramu v | Admin Activity | 02 Aug, 2017 08:36:23 EDT |
| Management Console Login | LOCAL | ramu v | Admin Activity | 02 Aug, 2017 08:21:49 EDT |
| Management Console Login | LOCAL | ramu v | Admin Activity | 02 Aug, 2017 07:35:34 EDT |
| Management Console Login | LOCAL | ramu v | Admin Activity | 02 Aug, 2017 07:09:50 EDT |
| Management Console Login | LOCAL | ramu v | Admin Activity | 02 Aug, 2017 04:46:34 EDT |
| Management Console Login | LOCAL | ramu v | Admin Activity | 01 Aug, 2017 08:42:39 EDT |

Previous Page (1/4) Next

The Event Log List view displays the following columns:

| Search Elements Properties | Description |
|----------------------------|--|
| Actions | Displays a list of all the actions that are performed on devices, policies or device sets. |
| Object Type | Displays a list of the object types, for example Device, Policy or Device Set. The actions are performed on the specific object types. |
| Object Name | Displays a list of the object names. |
| Initiated By | Displays name of the administrators who initiated action on a device, policy or a device set. |
| Time Stamp | Displays a list with the duration and the time stamp. |

You can scroll the grid view through **Previous** the **Next** button. You can perform the following activities from this page:

- [Search Event Log](#)

6.12.1 Search Event Log

You can search a required action carried out on a device, device set or policy through search filters based on all the grid columns. You can apply a single or a combination of search filters to define the search criteria and get the refined outcome. To search for an action, follow these steps:

| Action ▼ | Object Type | Object Name | Initiated By | Time Stamp |
|--|-------------|---|--|---|
| <input type="text" value="Search Action"/> | All ▾ | <input type="text" value="Search Object Name"/> | <input type="text" value="Search Initiated By"/> | <input type="text" value="Start Time"/> <input type="text" value="End Time"/> |
| Device Info | Device | U-1 google_sdk | akram ali | 02 Jan, 2014 06:04:52 EST |

1. Enter or select details for following search filters:
 - a. **Action:** Enter partial or complete action details in the **Search Action** text field.
 - b. **Object Type:** Select the required **Object Type** from the drop-down list. By default, it is set to All, which you can modify.

- c. **Object Name:** Enter partial or complete object name in the **Search Object Name** text field.
- d. **Initiated By:** Enter partial or complete name of the Administrator, who initiated the action.

The screenshot shows a 'Time Stamp' dialog box. At the top, there are two text input fields: the first contains '01/17/2014 00:00' and the second contains '01/23/2014 00:00'. Below these is a calendar for 'January 2014'. The calendar grid shows days of the week (Su, Mo, Tu, We, Th, Fr, Sa) and dates. The date '23' is highlighted in white, while other dates are in grey. Below the calendar, there is a 'Time' field showing '00:00'. Underneath are two sliders: 'Hour' and 'Minute', both with their sliders positioned at 0. At the bottom of the dialog are two buttons: 'Now' on the left and 'Done' on the right.

- e. **Time Stamp:** Time Stamp feature allows you to select a specific time period and view the actions performed into this time period.

This feature includes two fields. **Start Time** and **End Time**. Click in the Start Time field.

Calendar appears.

- f. Select the date. The selected date and the current time is updated in the **Start Time** field.
- g. Click **Done** to close the calendar.
- h. Repeat the same process to enter details for **End Time**.

2. According to your search filter criteria, the list view is updated with respective event log details. By default, the list view displays ten event logs according to default Display settings, which you can modify through **Display** dropdown list. You can also scroll the list view through **Previous** and the **Next** buttons.

6.13 System Status

The primary purpose of the System Status is to monitor the status of EMM components and monitor EMM jobs. For Installer version, Logging tab is provided to modify the log file mode such as debug mode with respect to the user requirements.

From the **Settings** section, click **System Status** from the left panel. The System Status page appears with three tabs.

- [Health Check](#)
- [Job Monitor](#)
- [Logging](#)
- [Wrap-Config](#)

For cloud version only Health Check and Job Monitor tabs are available. Logging tab is applicable only for installer version.

By default, health check validation happens periodically.

















6.13.1 Health Check

The primary purpose of Health Check is to display and monitor the current status of EMM components, on a single page. Admin can monitor the various components and ensure that they remain operational at all times.

System Status

Health Check
Job Monitor
Logging
Wrap-Config

Check all services (This may take up to 2-5 minutes)

| Service | Status | Effect |
|---|-------------|--------|
| Access to Directory servers  | Not checked | |
| Access to Apple Cloud  | Not checked | |
| Access to BES server  | Not checked | |
| Access to Database server  | Not checked | |
| Access to File Store  | Not checked | |
| Access to Exchange service  | Not checked | |
| Access to Google Cloud  | Not checked | |
| Webserver configuration  | Not checked | |
| Access to Mac server  | Not checked | |
| Access to Mail server  | Not checked | |
| Access to Memcache  | Not checked | |
| Access to SCEP server  | Not checked | |
| Access to Apple VPP server  | Not checked | |
| Access to Windows server  | Not checked | |
| Access to Windows 2003 server  | Not checked | |
| Access to WNS server  | Not checked | |

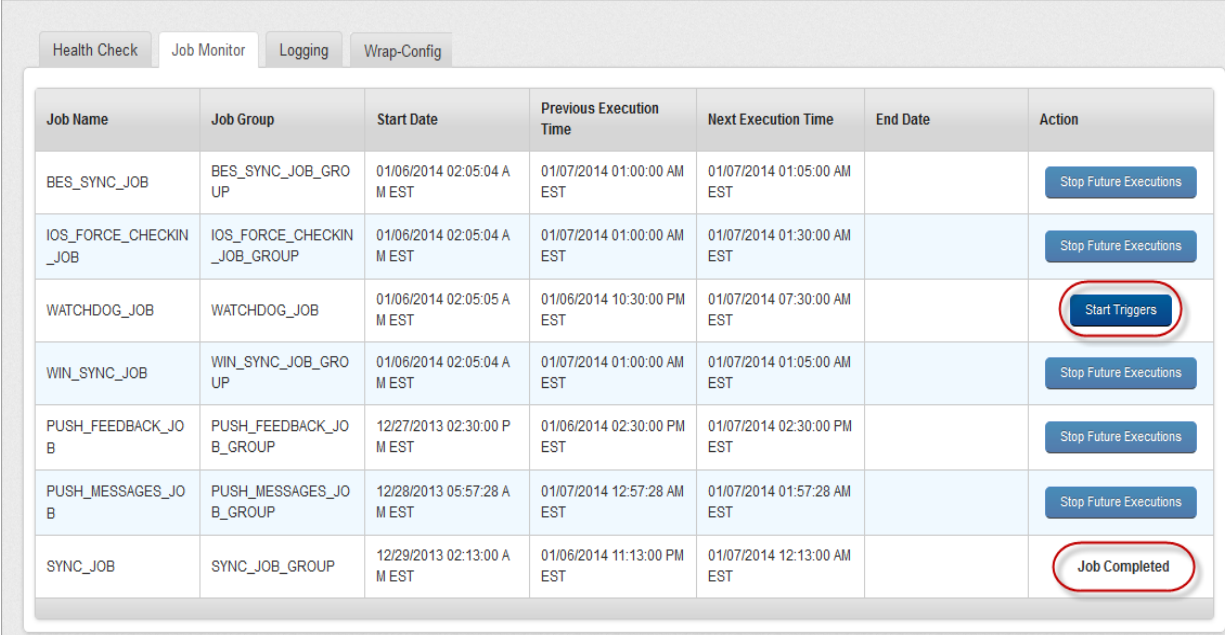
The health checking system runs internally on a periodic basis.

The Health Check list displays the following statuses:

| Status | Description |
|----------------|---|
| Passed | if the component interaction is successful, passed status is displayed. |
| Failed | if the component is not reachable, then failed status is displayed.. |
| Not Configured | If the component is not configured, then this status is displayed. |

6.13.2 Job Monitor

The primary purpose of the Job Monitor task is to quickly review the real time status of running jobs and take appropriate actions with respect to the requirements.



| Job Name | Job Group | Start Date | Previous Execution Time | Next Execution Time | End Date | Action |
|-----------------------|-----------------------------|----------------------------|----------------------------|----------------------------|----------|------------------------|
| BES_SYNC_JOB | BES_SYNC_JOB_GROUP | 01/06/2014 02:05:04 AM EST | 01/07/2014 01:00:00 AM EST | 01/07/2014 01:05:00 AM EST | | Stop Future Executions |
| IOS_FORCE_CHECKIN_JOB | IOS_FORCE_CHECKIN_JOB_GROUP | 01/06/2014 02:05:04 AM EST | 01/07/2014 01:00:00 AM EST | 01/07/2014 01:30:00 AM EST | | Stop Future Executions |
| WATCHDOG_JOB | WATCHDOG_JOB | 01/06/2014 02:05:05 AM EST | 01/06/2014 10:30:00 PM EST | 01/07/2014 07:30:00 AM EST | | Start Triggers |
| WIN_SYNC_JOB | WIN_SYNC_JOB_GROUP | 01/06/2014 02:05:04 AM EST | 01/07/2014 01:00:00 AM EST | 01/07/2014 01:05:00 AM EST | | Stop Future Executions |
| PUSH_FEEDBACK_JOB | PUSH_FEEDBACK_JOB_GROUP | 12/27/2013 02:30:00 PM EST | 01/06/2014 02:30:00 PM EST | 01/07/2014 02:30:00 PM EST | | Stop Future Executions |
| PUSH_MESSAGES_JOB | PUSH_MESSAGES_JOB_GROUP | 12/28/2013 05:57:28 AM EST | 01/07/2014 12:57:28 AM EST | 01/07/2014 01:57:28 AM EST | | Stop Future Executions |
| SYNC_JOB | SYNC_JOB_GROUP | 12/29/2013 02:13:00 AM EST | 01/06/2014 11:13:00 PM EST | 01/07/2014 12:13:00 AM EST | | Job Completed |

The Job Monitor list view displays the following columns:

| Column | Description |
|-------------------------|--|
| Job Name | Displays the job name. |
| Job Group | Displays the group to that job belongs. |
| Start Date | Displays the start date of the job. |
| Previous Execution Time | Displays the previous execution time of the job. |
| Next Execution Time | Displays the next execution time of the job. |
| End Date | Displays the end date of the job, if applicable. |
| Action | Displays the current action executed on a job. |

You can perform the following activities from the Job Monitor page:

- [Stop Future Execution](#)

6.13.2.1 Stop Future Execution

Based on requirement, the Admin may stop a job from further execution.

To stop a job, follow these steps;

1. Click the **Stop Future Execution** button under Action column.
Start Triggers button appears. This indicates that job execution is stopped.
2. To resume the job execution, click the **Start Triggers** button.

Jobs that are already triggered and in progress cannot be stopped, and the server waits for the completion of the job. Once already initiated job is completed, the status is displayed as Jobs Completed in the list view.

Important: For `IOS_FORCE_CHECKIN_JOB`, if you disable the job monitor by clicking Stop Future Execution, when you change device settings in the Kony Management administrator console, the `IOS_FORCE_CHECKIN_JOB` is enabled again.

6.13.3 Logging

Logging is supported for installer version only.

The server logs are created with respect to activities initiated on the server and maintained automatically. This server log page maintains history of services, exceptions, and warnings encountered during activities. Based on a user requirement, the admin can modify the current log level info generated in the server log.

The screenshot shows the 'System Status' page with the 'Logging' tab selected. It displays a table of loggers and their current log levels. A dropdown menu is open for the 'Log Level' column, showing the following options: WARN, INFO, DEBUG, ERROR, WARN (selected), OFF, and FATAL. The table lists the following loggers:

| Log Name | Log Level |
|---|-----------|
| com.amazonaws.services.s3 | WARN |
| com.amazonaws.http.IdleConnectionReaper | WARN |
| com.amazonaws.http.HttpClientFactory\$LocationHeaderNotRequiredRedirectStrategy | WARN |
| com.amazonaws.http.AmazonHttpClient | WARN |
| com.googlecode.hibernate.memcached | WARN |

The Logging level column displays the following log level options.

| Log Level | Description |
|-----------|--|
| Warn | Information that can be useful for debugging problems. |

| Log Level | Description |
|-----------|--|
| Debug | Information that is helpful to resolve any type of issues. |
| Error | Information that can be useful for debugging problems. |
| Off | Disables the log level. |
| Fatal | An error that causes a service to abort. |

Based on the user requirement Admin can modify the log levels.

6.13.4 Wrap-Config

The Wrap-Config tab provides details about Android wrapping configuration tools in the EMM console.

An administrator can view all Android wrapping tool versions in the EMM management console by clicking the **Check for Versions** button in the **Wrap-Config** tab.

System Status

The screenshot shows the 'Wrap-Config' tab selected in a navigation bar. Below the navigation bar, there is a section titled 'Android Wrapping Configuration Tools' with a 'Check for Versions' button. A table below the button lists the versions of three tools:

| Android Wrapping Configuration Tools | |
|--------------------------------------|------------------------------------|
| Check for Versions | |
| AAPT Tool Version | Android Asset Packaging Tool, v0.2 |
| APK Tool Version | 2.0.0 |
| Dexguard Version | DexGuard, version 6.1.04 |

7. Access Management

The primary purpose of Access Management is to manage users, user-groups, permission sets and track user activity. Administrators perform varied tasks like activating or deactivating a user, sync selected users, and apply permission set to groups to maintain application security.

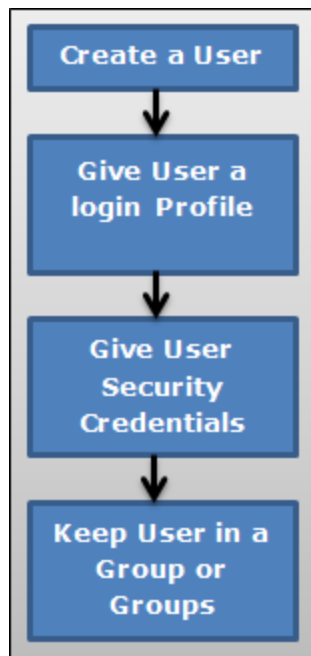
7.1 Managing Access

Access management includes:

- [User Management](#)
- [Group Management](#)
- [Permission Set](#)

7.2 Users

A user is an individual person. Each user needs an account to access the EMM Console. Administrator creates a user account for each person who uses the EMM Console.



The process to create a new User is as follows:

1. Create a new user.
2. Provide details for the user settings so that the user can access the account.
3. Save the configuration details.
4. A new user is created at the end of this activity.
5. A new user is assigned to a Group or Groups (Optional). By default, any new user is part of the **All** group.

From the **Access Management** tab, click **User**. The Users screen appears with the list of users. The list view displays a list of all the users along with other details. You can search the users based on each column.

Users

[+ New User](#)
[Import Users](#)

Displaying 1 - 2 of 2 - Display

| <input type="checkbox"/> | Display Name | User ID | Source Type | Source | Email | Status | Permission Set |
|--------------------------|---|--|---|--|--|---|--|
| | <input type="text" value="Search Users"/> | <input type="text" value="Search Username"/> | <input type="text" value="All Source Types"/> | <input type="text" value="All Sources"/> | <input type="text" value="Search Emails"/> | <input type="text" value="All Statuses"/> | <input type="text" value="All Permission Sets"/> |
| <input type="checkbox"/> | afw | afw | Local Reset Password | NA | afw@kony.com | Active | None |
| <input type="checkbox"/> | admin | admin | Local Reset Password | NA | admin@kony.com | Active | Admin Permissions |

[Sync Selected Users](#)
[Activate](#)
[Deactivate](#)
[Delete](#)
[Previous](#) **Page {1/1}** [Next](#)

- Represents Users Under Moderation.

The Users list view displays the following columns:

| Column | Description |
|-----------------|--|
| Select checkbox | <p>If selected at row level, the particular user is selected for any further actions. Multiple rows can also be selected.</p> <p>Selection can only be done on a single page of records. You can choose to display upto 100 records (users).</p> |
| Display Name | Displays the name defined for display for the user. |
| User ID | Displays the User ID of the user. |
| Source Type | Displays if the user is imported from the Active Directory or created Locally or imported from Kony Fabric. |
| Source | Displays source that belongs to user. If it is a local user, the system displays as NA |
| Email | Displays the email ID as received from the Active Directory or as specified by the Admin. |

| Column | Description |
|---------------------|--|
| Status | Displays the Status as received from the Active Directory or as specified by the Admin. |
| Permission Set | Displays the Permission Set as specified by the Administrator. Note: Administrators with limited access can only view permission sets assigned to them by a super administrator. |
| Sync Selected Users | Selected Users can be synchronized from Active Directories to get the latest details of users. This button is only active if the check box next to Display Name is selected or if the multiple select check box is selected. |
| Activate | Selected users can be activated. This button is only active if the check box next to Display Name is selected or if the multi select check box is selected. |
| Deactivate | Selected users can be deactivated. This button is only active if the check box next to Display Name is selected or if the multi select check box is selected. |
| Delete | Selected users can be deleted. This button is only active if the check box next to Display Name is selected or if the multi select check box is selected. |

You can navigate the list view through the **Previous** and the **Next** buttons.

You can perform the following activities from the User page:

- [Creating a New User](#)
- [Importing Users from the Active Directory](#)
- [Automatic Creation of a New User Using Kony Fabric Data](#)
- [Searching for Users](#)
- [Updating a User](#)
- [Sync Selected Users](#)

- [Activating a User](#)
- [Deactivating a User](#)
- [Deleting a User](#)

7.2.1 Creating a New User

Only an administrator can add a User to the EMM database.

By default, any new user is part of the **All** group.

To create a new User, follow these steps:

1. To create a new user, click the **+ New User** button next to the **User** label at the top of the page.



Add New User window appears.

2. Enter details for the following fields:
 - a. **First Name:** Enter the First Name of the user.
 - b. **Last Name:** Enter the Last Name of the user.
 - c. **Display Name:** Enter a user name. This is a unique name to identify a user.
 - d. **Email:** Enter the email address of the user. It can include alphanumeric and special characters that follow standard email address representation.
 - e. **Phone:** Enter phone number of the user. It should be numeric. You can also use + to as a prefix for the country code.

- f. **User ID:** Enter the User ID of the user. Its length can vary from 1-500 characters including alphanumeric and special characters. You cannot create user IDs with Special characters such as / \ [] : ; | = , + * ? < > @ "
- g. **Password:** Enter the password for the user. This is a string of characters that allows access to a system. It can be a combination of alphanumeric, numeric, and special characters.
- h. **Confirm Password:** Retype the password to acknowledge with definite assurance.

Important: While creating a User, in the **Password** and the **Confirm Password** fields all the leading and trailing space characters are removed.

- i. **Active:** By default, a newly created user is active. The newly created user appears as an active user in the list view under Status column. You can deselect the check box to create an inactive user.
 - j. **Enrollment Mode:** Select an enrollment mode from the list. For more information on different enrollment modes and their impact on available features in the Kony Management Suite, refer [Enrollment Mode](#).
3. Click the **Save** button to save the details. In the confirmation message that appears, click **OK** to continue.

The newly added user appears in the list view.

Note: Fields with the red asterisk sign are mandatory.

7.2.2 Importing Users from the Active Directory

An Active Directory (AD) is a centralized and standardized system that automates network management of user data. You can also add users to the EMM database by importing them from the ADs by using **Import Users** window.

By default, any new user is part of the **All** group.

The users thus imported appears in the Users List page and apps can be targeted towards them.

Before initiating a new request to import Users, as an Admin you must meet the following conditions:

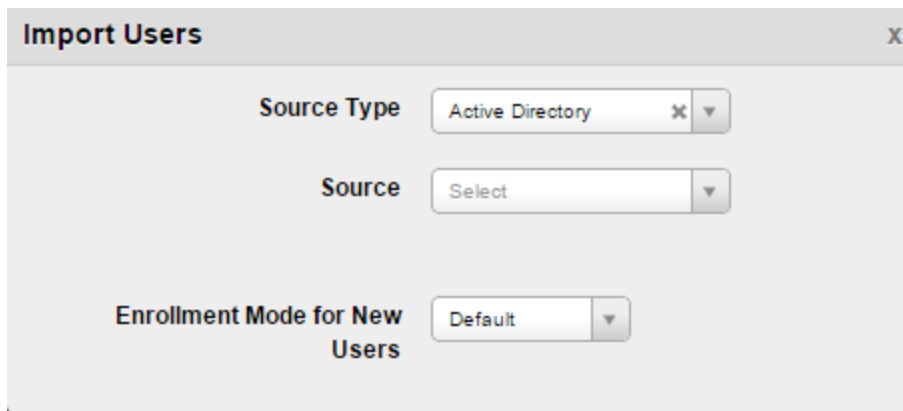
- Ensure that any of the sync jobs is not in progress. If no sync jobs in progress, then only you can request for importing Users.
- If sync is in progress, the Sync All and Sync Imported buttons are deactivated and are not available for Admin to do adhoc sync.

To import a user from Active Directory, follow these steps:

1. To import a new user, click the **Import Users** next to the User label at the top of the page.

The **Import Users** window appears with Source Type drop-down list.

2. Select the source type from the **Source Type** list. Available source type details appear.
3. Select **Active Directory**. **Source** list appears.



The screenshot shows a dialog box titled "Import Users" with a close button (X) in the top right corner. Inside the dialog, there are three dropdown menus:

- Source Type**: A dropdown menu with "Active Directory" selected and a close button (X) on the right.
- Source**: A dropdown menu with "Select" selected.
- Enrollment Mode for New Users**: A dropdown menu with "Default" selected.

4. Select the source from the Source list.
5. Select an enrollment mode from **Enrollment Mode for New Users** list. For more information on different enrollment modes and their impact on available features in the Kony Management Suite, refer to the [Enrollment Mode page](#).
6. You can search for the users through the available search filters. Apply a single or a combination of search filters to define the search criteria and get the refined outcome.

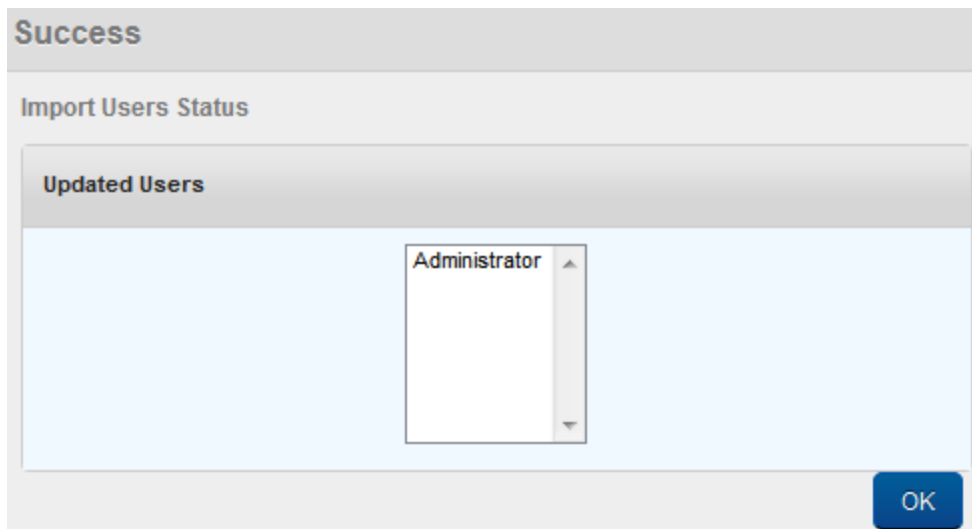
- a. **AD Username:** Enter partial or complete name of the user in the Search Username field.
- b. **First Name Last Name:** Enter partial or complete display name of the user in the Search Display Name field.
- c. **Email:** Enter email address of the user in the Search Emails field.
- d. **Phone Number:** Enter phone number of the user in the Search Phone field.

Based on the search criteria, the list view is updated with respective user details. You can navigate the list view using the **Previous** and the **Next** buttons.

7. Select the required user or users through the check box next to **AD Username** listing. You can select the complete user list by selecting the check box next to the **AD Username** column name.

Important: You can also import a user without an email ID.

8. Click the **Import** button to import the users from the Active Directory. The System displays the **Success** Window with a list of the updated users.



9. Click the **OK** button to return to the main page.

7.2.3 Automatic Creation of a New User Using Kony Fabric Data

When the Kony Fabric identity Service is configured, if the Kony Fabric user does not exist in the Kony Management server, a new user is created (in Kony Management server) automatically using the data from Kony Fabric identity service. An administrator does not have any role in creating a user based on information from Kony Fabric.

- Information is gathered from the MFToken, and the user is created in the Kony Management server.
- If the MFToken does not have any user information, Kony Management server will throw an exception and the Enterprise Store will provide a **login failed** response.
- If a user is created using the MFToken, the **Reset Password** button will not display on the Enterprise Store and Kony Management Administrator console. This is because a user, who is created using MFToken information will not have a password in Kony Management Suite.
- A user created using an MFToken will not be able to log into the Kony Management self-service console.
- If a local user with the same name exists in Kony Management server as that of the MFToken user, MFUser is added to the user ID.
- If the Overwrite local user with imported user option is configured to **Yes**, and if users are imported from Active Directory group, Kony Fabric user is overridden by an Active Directory user. But on next login call, Kony Fabric user is created again.

7.2.4 Searching for Users

You can search for the users through the available search filters. Apply a single or a combination of search filters to define the search criteria and get the refined outcome.

Users

+ New User

Import Users

Displaying 1 - 2 of 2 - Display

| <input type="checkbox"/> | Display Name | User ID | Source Type | Source | Email | Status | Permission Set |
|--------------------------|---|--|---|--|--|---|--|
| | <input type="text" value="Search Users"/> | <input type="text" value="Search Username"/> | <input type="text" value="All Source Types"/> | <input type="text" value="All Sources"/> | <input type="text" value="Search Emails"/> | <input type="text" value="All Statuses"/> | <input type="text" value="All Permission Sets"/> |
| <input type="checkbox"/> | afw | afw | Local Reset Password | NA | afw@kony.com | Active | None |
| <input type="checkbox"/> | admin | admin | Local Reset Password | NA | admin@kony.com | Active | Admin Permissions |

Page {1/1}

- Represents Users Under Moderation.

1. Enter or select details for the following search filters:
 - a. **Display Name:** Enter partial or a complete display name in the **Search Users** field.
 - b. **User ID:** Enter partial or a complete User ID in the **Search Username** field.
 - c. **Source Type:** Select the desired option from the drop-down list, for example, Active Directory.
 - d. **Source :** Select the desired option from the drop-down list.
 - e. **Email:** Enter email address of the user in the **Search Emails** field.
 - f. **Status :** Select the desired option from the drop-down list, for example, Active or Inactive.
 - g. **Permission Set:** Select the desired option from the drop-down list.

2. The list view is updated with respective user details, as per the search criteria.

By default, the list view displays ten users according to Display settings that you can modify through the **Display** drop-down list. You can also scroll the list view through **Previous** and the **Next** button.

7.2.5 Updating a User

Administrators need to update details of the local users and users imported from active directory for various reasons like applying permission sets or assigning a user to a user group.

You may require to update details of the users from the following sources:

- [Local User](#)
- [Active Directory](#)
- [Cloud](#)

7.2.5.1 Local User

To update a local user details, follow these steps:

1. Select the user source as Local from the list view.

A list of local users appears in the list view.

2. Click the required user in the list view that you need to update.

The User Details page appears.

3. The User Details page includes three sections
 - User Details
 - Groups
 - Permissions

User Details

Users > Anupam

Permission Set Applied: None

User Details

| | |
|-------------------|---|
| User ID | bipin |
| First Name | <input type="text" value="Bipin"/> |
| Last Name | <input type="text" value="Jethwani"/> |
| Display Name * | <input type="text" value="Bipin Jethwani"/> |
| Email * | <input type="text" value="bipin.jethwani@kony.com"/> |
| Phone | <input type="text" value="+XXXXXXXXXXXX"/> |
| Active | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Unlock | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Custom Attributes | <input type="text" value="Select Custom Attribute"/> |
| Enrollment Mode | <input type="text" value="Default"/> |
| Enterprise Store | <input type="text" value="Select Enterprise Store"/> |

4. **User Details:** The User Details section includes First Name, Last Name, Display Name, Email and Phone fields. The fields are populated by local user details. You can update these details.

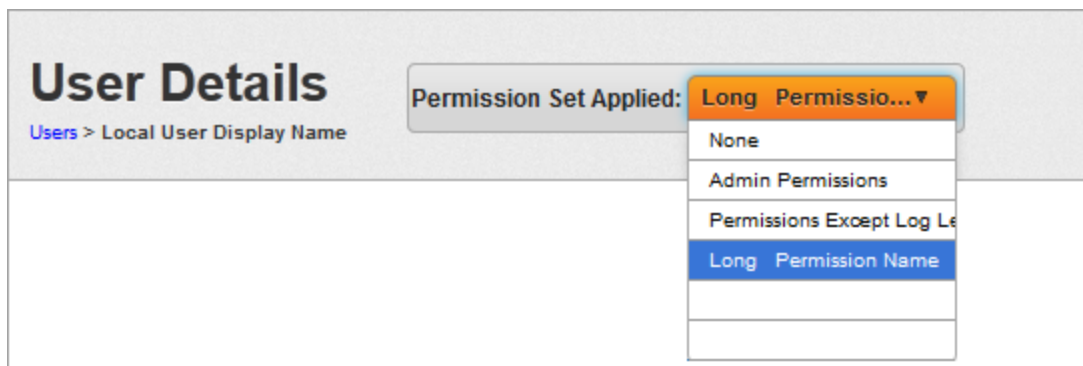
By default, the user status is set to active. If required, you can change the user status to inactive.

The **Unlock** feature will control the user's access to the Enterprise Appstore. However, if the user is locked by the backend (for example Active Directory) used for authentication, user will not be able to log in.

Important: If your external authentication failed attempts count is configured to X, the Lock After feature in the Usage Settings (Application Settings page) should be less than or equal to X. When you are using an external authentication mechanism Kony Management only passes on the request for authentication.

You can add custom attributes to the user from the custom attributes list. Select an enrollment mode from **Enrollment Mode** list. For more information on different enrollment modes and their effect on features in Kony Management Suite, refer to the [Enrollment Mode](#). Select an Enterprise Store from the Enterprise Store list.

5. **Groups:** Enter the name of the group you want to assign the user.



6. **Permission Set:** Select the required permission set from the **Permission Set Applied** dropdown list.

The updated User details with applied permission set appear in the list view.

You can also apply a Permission set to a user from the main page.

7. To apply a Permission set to a user from the list view, follow these steps:

| <input type="checkbox"/> | Display Name | User ID | Source | Email | Status | Permission Set |
|--------------------------|---|--|------------------|--|----------------|---|
| | <input type="text" value="Search Users"/> | <input type="text" value="Search Username"/> | All Sources ▾ | <input type="text" value="Search Emails"/> | All Statuses ▾ | All Permission Sets ▾ |
| <input type="checkbox"/> | sandeep.n. | sandeep26 | Active Directory | sandeep26@mdmtest.local | Active | <div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">None ▾</div> <div style="padding: 2px;">None</div> <div style="padding: 2px;">Admin Permissions</div> <div style="padding: 2px;">Permissions Except Log Level</div> <div style="padding: 2px;">Long Permission Name Te</div> </div> |

- a. Select the required Permission set from the list view and then click **Save**. A success message appears. Click **OK** to return to the main page.

8. Click the **Save** button to save the details.

9. In the confirmation message that appears, click **OK** to return to the main page.

Reset Password

Important: EMM Installation comes with default user 'admin'. Please do not change its permission set to 'None'. If you change the permission set, admin user can not log on to the EMM administration console.

1. Select the user state as Local from the list view.

A list of local users appears in the list view.

2. Click the **Reset Password** button for the user, you wish to reset the password.

Reset Password

New Password *

Confirm Password *

Reset Password window appears.

3. **New Password:** Enter the new password. The new password should be a combination of alphanumeric characters.

4. **Confirm Password:** Retype the password to confirm it.

A confirmation message about password acceptance appears.

5. Click the **Save** button to save the new password.

A confirmation message about password update appears.

7.2.5.2 Users imported from Active Directory

To update a user from Active Directory, follow these steps:

| <input type="checkbox"/> | Display Name | User ID | Source Type | Source | Email | Status | Permission Set |
|--------------------------|---|--|--------------------|---------------|--|----------------|-----------------------|
| | <input type="text" value="Search Users"/> | <input type="text" value="Search Username"/> | All Source Types ▲ | All Sources ▼ | <input type="text" value="Search Emails"/> | All Statuses ⇅ | All Permission Sets ⇅ |
| <input type="checkbox"/> | | | All Sources | | | Active | india fm ▼ |
| | | | Local | | | | |
| | | | Active Directory | | | | |
| | | | SAP HCM | | | | |

1. Select the user source type as Active Directory from the list view.

A list of Active Directory users appears in the list view.

2. Select the required user from the list.

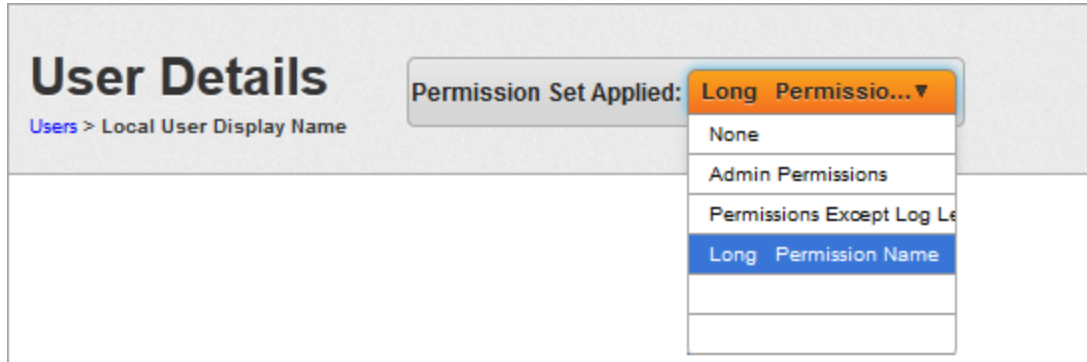
User Details page appears.

The User Details page includes three sections - User Details, Groups and Permissions.

User Details section includes **First Name**, **Last Name**, **Display Name**, **Email** and **Phone** fields. These fields are populated by already existing active directory user details. You cannot update AD user details.

To assign AD user to a group and apply the required policy, follow these steps:

1. **Groups:** You can assign an AD user to the required group. You can search the required Group by entering partial or complete Group name in the Search field.



2. **Permission Set:** Select the required permission set from the **Permission Set Applied** drop-down list.

The updated User details with applied permission set appear in the list view.

3. Click the Save button to save the details.
4. In the confirmation message that appears, click **OK** to return to the main page.

The following table provides additional information about Permission Set:

| Properties | Description |
|----------------|--|
| Permission Set | <ul style="list-style-type: none"> • When you assign a User to a Group, the user inherits all the permission sets applied to that group automatically. • When you assign a user with a permission set, the user behaves as per the applied permission set, when user logs-in into the Management Console. The applied permission set overrides the group permission set. • When you remove the applied permission set of a user, then group permission sets are applied to that user automatically. • When a User is removed from a group, then all the applied permission sets applied through the group are removed automatically. |

7.2.5.3 Cloud

Admin can create users with admin privileges for cloud environment. The created user can login into EMM Management Console through cloud login credentials.

7.2.6 Sync Selected Users

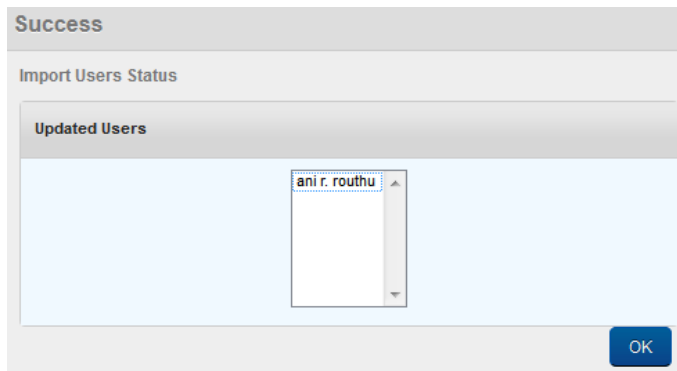
This action synchronizes all the User details including any new or removed associations with any Group or Groups. The Admin can choose to synchronize an individual user or multiple users at a time by selecting check boxes on the left of each User and clicking **Sync Selected Users**. This action synchronizes all the details of the Users including any new or removed associations with any Groups. This action is applicable to AD Users.

Note: Synchronizing Users applies only to Users from multiple ADs. It does not apply to local Users.

| | | | | | | | |
|-------------------------------------|-------------------|-------------------|-----|----------------------------|--|--------|--------|
| <input checked="" type="checkbox"/> | Akramali Mohammad | akramali.mohammad | ADS | akramone@mdmtest.local | | Active | none ▼ |
| <input checked="" type="checkbox"/> | ani r. routhu | anil.routhu | ADS | anil.routhus@mdmtest.local | | Active | none ▼ |

To Sync the selected users, follow these steps:

1. Select the required User or Users from the list view. The **Sync Selected Users** button becomes active.
2. Click the **Sync Selected Users** button. The System displays the **Success** window with a list of the updated users.



3. Click the **OK** button to return to the main page.

7.2.7 Activating/Deactivating a User

If a User is deleted in the Active Directory, then the user should be deactivated in the EMM Access Management. The User cannot be active and should be removed from all the Groups. When a user is deactivated, user will not be allowed to login to the enterprise store.

Important: When any of the users (Local or AD) is deactivated, the user's association with the All group is removed. Once the user is activated again, the user is automatically added to the All group again.

If the User as an Admin created any entities, the user is still credited with the same entities - Applications, categories, and MAM policies. No other references of the User persist in the EMM system.

To change the status to Active or Deactive for a User, follow these steps:

1. To activate or deactivate a user, select the user and click **Active** or **Deactivate** at the bottom of the User page.

The **Activate** or **Deactivate Action** dialog appears asking, if the user status be activated/deactivated.

| <input type="checkbox"/> | Display Name | User ID | Source Type | Source | Email | Status | Permission Set |
|-------------------------------------|---|--|---|--|--|---|--|
| | <input type="text" value="Search Users"/> | <input type="text" value="Search Username"/> | <input type="text" value="All Source Types"/> | <input type="text" value="All Sources"/> | <input type="text" value="Search Emails"/> | <input type="text" value="All Statuses"/> | <input type="text" value="All Permission Sets"/> |
| <input checked="" type="checkbox"/> | user4 | user4 | SAP HCM | Sample | sss | Active | None |

2. Click **OK** to continue. A confirmation message about activated/deactivated user status appears.

The system changes the state of the User to Active/Inactive.

7.2.8 Deleting a User

To delete a user, follow these steps:

1. To delete a user, select the user and click **Delete** at the bottom of the User page.

The **Delete Action** dialog appears asking, if the user can be deleted.

| <input type="checkbox"/> | Display Name | User ID | Source Type | Source | Email | Status | Permission Set |
|-------------------------------------|---|--|---|--|--|---|--|
| | <input type="text" value="Search Users"/> | <input type="text" value="Search Username"/> | <input type="text" value="All Source Types"/> | <input type="text" value="All Sources"/> | <input type="text" value="Search Emails"/> | <input type="text" value="All Statuses"/> | <input type="text" value="All Permission Sets"/> |
| <input checked="" type="checkbox"/> | user4 | user4 | SAP HCM | Sample | sss | Active | None |

2. Click **OK** to continue. A confirmation message about deletion appears.

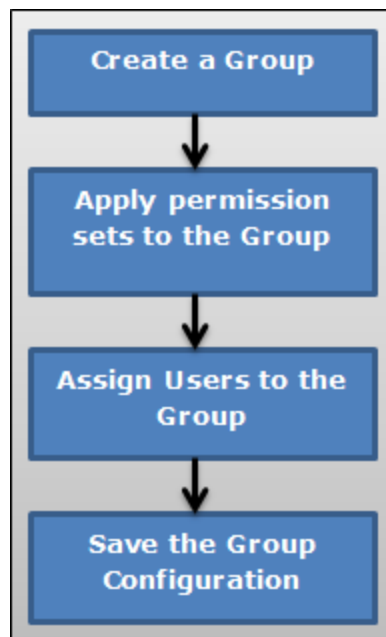
The system deletes the user from the grid.

When you delete a user, if there is a device enrollment request for an associated device, the device enrollment status will change from **Request Sent** to **Request Deleted**.

Important: When any of the users (Local or AD) is deleted, the user's association with the All group is removed.

7.3 Groups

Groups represent a collection of users created to provide security options for domains and other business services. Using the permission sets, you can grant or deny a group access to one or more domains, or set privileges for individual services. In all, a group represents multiple users with the same requirement and authority to access particular business services.



The process to create a new Group is as follows:

1. Create a new Group.
2. Apply Permission Set to the Group.
3. Assign user/users to the Group.
4. Save the configuration details.
5. A new Group is created at the end of this activity.

From the **Access Management** tab, click **Groups**. The Groups screen appears with the list of groups. The list view displays a list of all the groups along with other details. You can search the groups based on each column and also sort on each column.

Groups

[+ New Group](#)
[Import From Active Directory](#)

Displaying 1 - 4 of 4 - Display

| <input type="checkbox"/> | Group Name | Source Type | Source | Description | Status | Permission Set |
|--------------------------|--|---|--|---|---|--|
| | <input type="text" value="Search Groups"/> | <input type="text" value="All Source Types"/> | <input type="text" value="All Sources"/> | <input type="text" value="Search Description"/> | <input type="text" value="All Statuses"/> | <input type="text" value="All Permission Sets"/> |
| <input type="checkbox"/> | All | Local | NA | System generated group compris... | Active | <input type="text" value="None"/> |
| <input type="checkbox"/> | Sample_Medium | Local | NA | Sample group for Medium device... | Active | <input type="text" value="None"/> |
| <input type="checkbox"/> | Sample_High | Local | NA | Sample group for High device r... | Active | <input type="text" value="None"/> |
| <input type="checkbox"/> | Sample_Low | Local | NA | Sample group for Low device re... | Active | <input type="text" value="None"/> |

- Represents Groups Under Moderation.

By default, an **All** group is created when Kony Management suite is newly installed or upgraded from a previous version. The **All** group consists of all active users who exist in the Kony Management server. During an upgrade, if a group with name **All** exists at the time of the upgrade, **All_SystemGenerated** group is created. All active system users at the time of the upgrade will automatically be added to the **All_SystemGenerated** group.

Any new user created or imported in Kony Management server will automatically be added to the **All** group. The **All** group cannot be deleted by anyone. Even the administrators cannot delete or modify the all group. Using the all group, you can target any apps, MDM policies, and MCM content to all users.

You can not create groups with names **Sample_Medium**, **Sample_High**, and **Sample_Low** as these group names are reserved.

You can navigate the list view through the **Previous** and the **Next** buttons.

The Groups list view displays the following columns:

| Columns | Description |
|----------------------|---|
| Select checkbox | <p>If selected at row level, the particular group is selected for any further actions. Multiple rows can also be selected.</p> <p>Selection can only be done on a single page of records. You can choose to display upto 100 records (groups).</p> |
| Group Name | Displays the name of the group. You can use a hyphen in the name of the group. All other special characters are not allowed in the name of the group. |
| Source | Displays if the Group is imported from Active Directory or created Locally. |
| Domain | Displays domain that belongs to Group. |
| Description | Description of the Group detailing features and functionality. |
| Status | Displays the Status as received from the Active Directory or as specified by the Admin. |
| Permission Set | <p>Displays the Permission Set as specified by the Administrator.</p> <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p>Note: Administrators with limited access can only view permission sets assigned to them by a super administrator.</p> </div> |
| Sync Selected Groups | Selected Groups can be synchronized from Active Directories to get the latest details of groups. This button is only active if the check box next to Display Name is selected or if the multi-select check box is selected. |
| Activate | Selected groups can be activated. This button is only active if the check box next to Display Name is selected or if the multi select checkbox is selected. |
| Deactivate | Selected groups can be deactivated. This button is only active if the check box next to Display Name is selected or if the multi select checkbox is selected. |

| Columns | Description |
|---------|---|
| Delete | Selected groups can be deleted. This button is only active if the check box next to Display Name is selected or if the multi select checkbox is selected. |

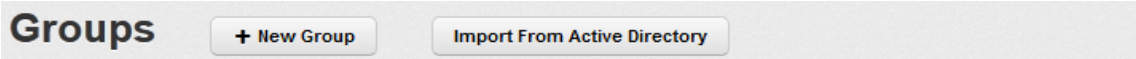
You can perform the following activities from the Groups page:

- [Creating a New Group](#)
- [Importing Groups from the Active Directory](#)
- [Searching for Groups](#)
- [Updating a Group](#)
- [Sync Selected Group](#)
- [Deactivating a Group](#)
- [Deleting a Group](#)

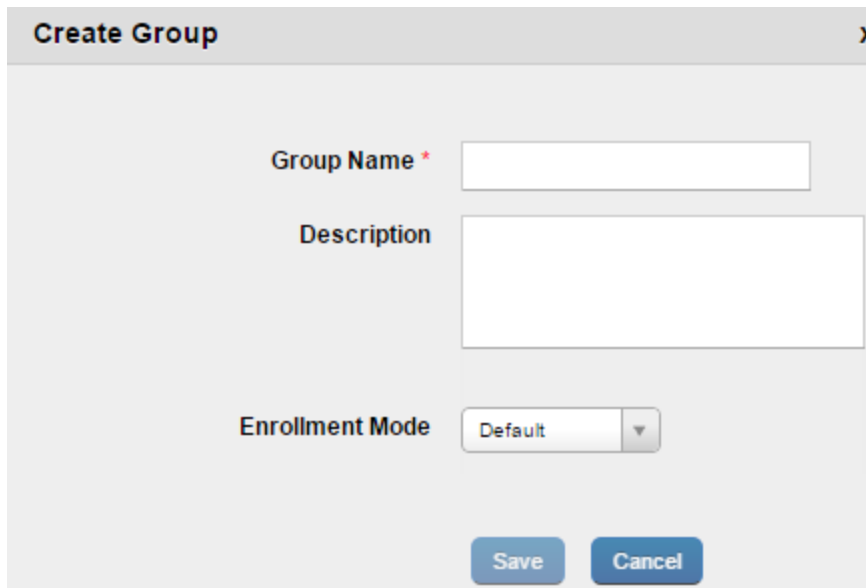
7.3.1 Creating a New Group

Only an Admin can add a Group to the EMM database.

To create a new Group, follow these steps:



1. To create a new Group, click the **+ New Group** button next to the **Groups** label at the top of the page.



The screenshot shows a 'Create Group' dialog box with the following fields and controls:

- Group Name ***: A single-line text input field.
- Description**: A multi-line text input area.
- Enrollment Mode**: A dropdown menu with 'Default' selected.
- Buttons**: 'Save' and 'Cancel' buttons at the bottom.

The **Create Group** window appears.

2. Enter details for the following fields:
 - a. **Group Name**: Enter an appropriate name for the Group.
 - b. **Description**: Enter an appropriate description of the group that clearly indicates its objective. You cannot create group names with Special characters such as `/ \ [] : ; | = , + * ? < > @` ". You can use a hyphen in the name of the group.
3. Select an enrollment mode from **Enrollment Mode** list. For more information on different enrollment modes and their impact on available features in the Kony Management Suite, refer to the [Enrollment Mode](#) page.
4. Click the **Save** button to save the details. In the confirmation message that appears, click **OK** to continue. By default, the newly created Group appears as active with no permission set applied on it in list view.

Click the **Cancel** button to close the window.

7.3.2 Importing Groups from the Active Directory

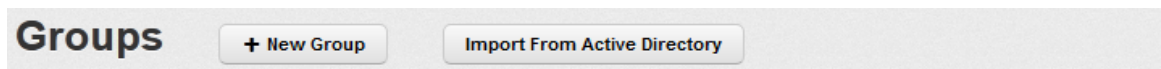
You can also add groups to the EMM database by importing them from the Active Directory, using the **Import Groups from Active Directory** window.

Note: Users imported into Kony Management Suite with this method (Importing Groups from Active Directory) will also be part of the default **All** group.

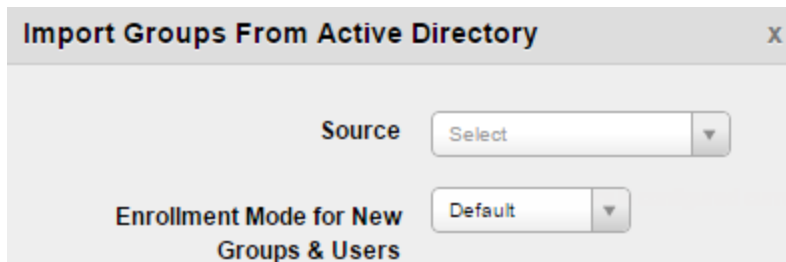
Important: If you move users from one Active Directory group to another, this may result in app un-targetting and re-targetting users who are moved.

To import a group from the Active Directory, follow these steps:

1. To import a new group, click the **+ Import From Active Directory** button next to the **New Group** button at the top of the page.



The **Import Groups from Active Directory** window appears with Domain drop-down list.



2. Select the group from the Source drop-down list. The Group details from the selected source appears in the grid.

Note: In case of Forest, the root domain is always the default context, and the system displays sub-domains of each Group against the Group names. For more details, refer to [AD Configuration](#).

Import Groups From Active Directory

Domain:

Displaying 1 - 25 of 212 - Display

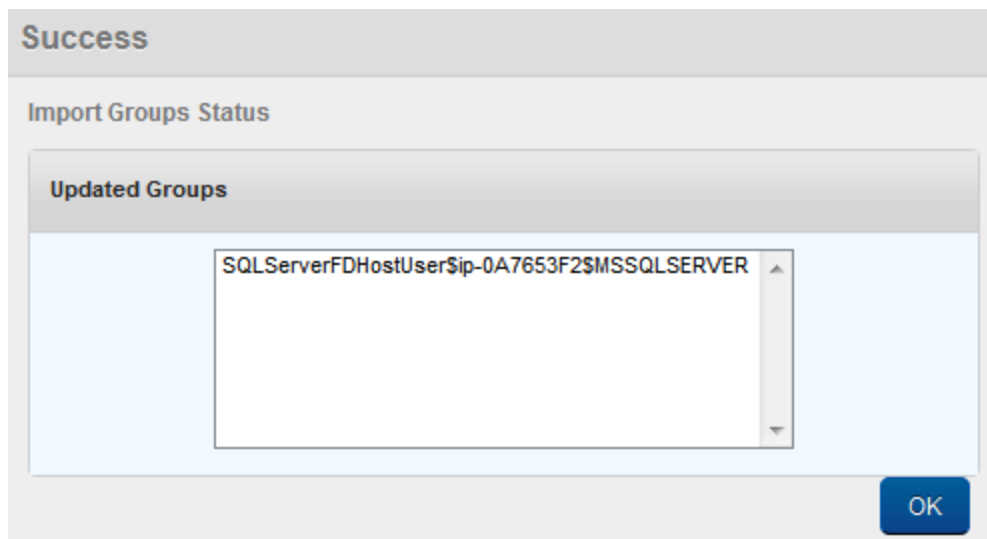
| <input type="checkbox"/> | Group Name | Email | Description |
|--------------------------|--|---|--|
| | <input type="text" value="AD Username"/> | <input type="text" value="Search Email"/> | <input type="text" value="Description"/> |
| <input type="checkbox"/> | Administrators | - | Global group for all android subscribers |
| <input type="checkbox"/> | Users | - | Global group for all androidGCM subsc... |
| <input type="checkbox"/> | Guests | - | Global group for all blackberry subsc... |
| <input type="checkbox"/> | Print Operators | - | Global group for all iphone subscribers |

Page {3/92}

3. Select an enrollment mode from **Enrollment Mode** list. For more information on different enrollment modes and their impact on available features in the Kony Management Suite, refer [Multi-license page](#).
4. You can search for the group through the available search filters. You can apply a single or a combination of search filters to define the search criteria and get the refined outcome.
 - a. **Group Name:** Enter partial or complete name of the group in the **Search Groups** field.
 - b. **Description:** Enter partial or complete description of the group in the **Search Description** field.

Based on the search criteria, the list view is updated with respective group details. You can navigate the list view using the **Previous** and the **Next** buttons.

5. Select the required group or groups through check box next to **Group Name**. You can select the complete group list by selecting the check box next to the **Group Name** column.
6. When you select the Group or Groups, the **Import** button becomes active. Click the **Import** button to import the groups from the Active Directory. The System displays the **Success** Window with a list of the updated groups.



7. Click the **OK** button to return to the main page. The Groups thus selected are copied to the EMM database and displayed in the Groups List page.

The following table provides additional information about Groups:

| Properties | Description |
|------------|--|
| Group Name | <p>Along with the Groups, all the Users that are part of the Group and part of any sub-groups are individually imported into the EMM system.</p> <ul style="list-style-type: none"> The sub-group itself is not imported and its details are not captured as a Group. For example, Group X includes a sub group named as Y. Group X has Users: A, B, C, D. Sub Group Y has users: A, F, G. When Group X is imported, all the six Users {A, B, C, D, F, G} are imported to the EMM system. Sub -Group Y is not imported. With the same example, if Sub-Group Y is imported, then only {A, F, G} are imported as Group Y is a sub-group. Only once the Groups are added, any apps can be targeted to them. |

7.3.3 Searching for Groups

You can search a desired group through the available search filters. You can apply a single or a combination of search filters to define the search criteria and get the refined outcome.

| <input type="checkbox"/> | Group Name | Source | Description | Status | Permission Set |
|--------------------------|--|--|---|---|--|
| | <input type="text" value="Search Groups"/> | <input type="text" value="All Sources"/> | <input type="text" value="Search Description"/> | <input type="text" value="All Statuses"/> | <input type="text" value="All Permission Sets"/> |
| <input type="checkbox"/> | Guests | Active Directory | Guests have the same access as... | Active | None |

- Enter or select details for following search filters:
 - Group Name:** Enter partial or complete name of the group in the **Search Groups** field.
 - Sources:** Select the desired option from the drop-down menu, for example, Local or Active Directory.

- c. **Description:** Enter partial or complete description of the group in the **Search Description** field.
2. The list view is updated with respective groups details, as per the search criteria. By default, the list view displays ten groups according to Display settings that you can modify through the **Display** drop-down list. You can also scroll the list view through **Previous** and the **Next** button.

7.3.4 Updating a Group

You may require updating group details for any reason such as applying permission sets. Admin can add Users to the Group by searching for them on the Users List. Groups can be created with the EMM created local Users and the AD Users. Groups can also be a combination of both the types of Users. When any app is targeted to a group, all the Users automatically get access to the same. Similarly, when a Permission set is applied to a Group, all the Users are granted the same permissions. You may require updating details of the groups through following sources:

- [Local Group](#)
- [Active Directory](#)

7.3.4.1 Local Group

To update a local group details, follow these steps:

| <input type="checkbox"/> | Group Name | Source | Description | Status | Permission Set |
|--------------------------|--|--|---|--------|--|
| | <input type="text" value="Search Groups"/> | <input style="border: 1px solid black; border-bottom: none; padding: 2px 5px;" type="text" value="All Sources"/> <div style="border: 1px solid black; border-top: none; padding: 2px 5px; margin-top: -1px;"> All Sources Local Active Directory Cloud </div> | <input type="text" value="Search Description"/> | Active | <input style="border: 1px solid black; border-bottom: none; padding: 2px 5px;" type="text" value="All Permission Sets"/> |

1. Select the group source as Active Directory from the list view.

A list of Active Directory groups appears in the list view.

2. Click the required group in the list view that you need to update. The **Group Details** page appears. The Group Details page includes three sections - Group Details, Users and

Permission Set Applied.

Group Details

Name Star Wars

Description ABC ✓

You have 483 characters left

Custom Attributes

Enrollment Mode

Enterprise Store

(Base Enterprise Store and others currently being signed cannot be targeted)

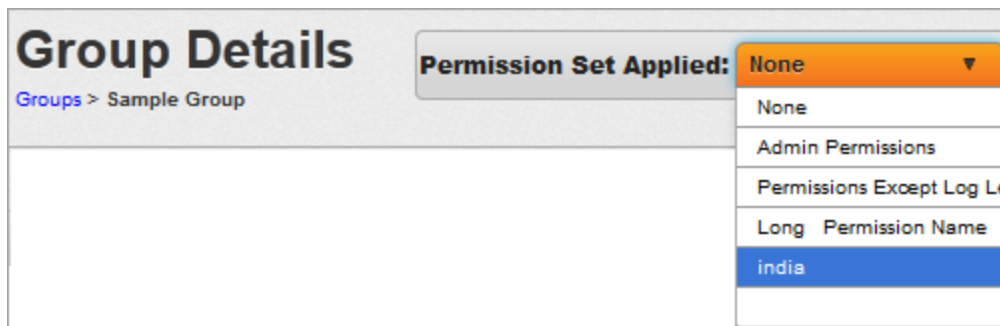
Users

[Add/Remove Users](#)

| Display Name | User ID | Source Type | Source |
|--------------|---------|------------------|--------|
| prem | prem | Active Directory | |

3. **Group Details:** This section is repopulated with existing Group details for the following fields.
 - a. **Name:** This field is pre-populated with the existing Group Name. You cannot modify the existing Group name.
 - b. **Description:**Based on requirement, you can update the particulars.
 - c. **Custom Attributes:** You can add Custom Attributes to the user from the Custom Attributes list.

- d. **Enrollment Mode:** Select an enrollment mode from **Enrollment Mode** list. For more information on different enrollment modes and their effect on available features in Kony Management Suite, refer to the [Enrollment Mode page](#).
 - e. **Enterprise Store:** Select an Enterprise Store from the Enterprise Store list.
 - f. **Custom Attributes:** You can add Custom Attributes to the user from the Custom Attributes list.
4. **Users:** Search the required user by entering the partial or complete user name in the Search field.
- a. To assign a user, use the left single-arrow icons to select the user.
 - b. To assign the complete user list, use the left double arrow icon.
 - c. To remove a user from the assigned list, select the right single arrow icon.
 - d. To remove all the users from the assigned list, click the right double arrow icon.
- **Assigned Users:** You can enter the name of a user to whom you want to assign the group.



5. **Permission Set:** Select the required permission set from the **Permission Set Applied** drop-down list. All the permissions granted in the permission set automatically is applied to all the users who are part of the Group.

You can also apply a permission set to a group from the main page. To apply a permission set to a group from the list view, follow these steps:

- a. Select the required permission set from the list view.
 - b. The Change Group Permission Set window appears asking, if the user wants to change the existing permission set. Click **OK** to continue
 - c. A confirmation message about changed permission set appears. Click **OK** to return to the main page.
6. Click the **Save** button to save the details.
 7. In the message that appears, click **OK** to return to the main page. The updated Group details with applied permission set appear in the list view.

7.3.4.2 Group imported from Active Directory

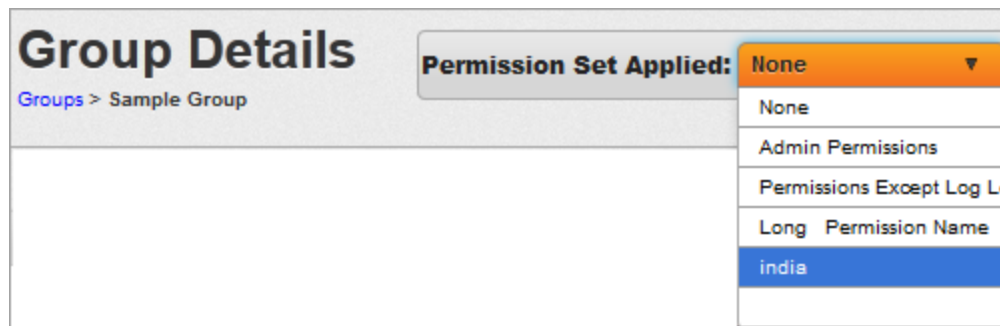
To update an Active Directory group, follow these steps:

| <input type="checkbox"/> | Group Name | Source | Description | Status | Permission Set |
|--------------------------|--|--|---|-------------------------------------|--|
| | <input type="text" value="Search Groups"/> | <input type="text" value="All Sources"/> <ul style="list-style-type: none"> All Sources Local Active Directory Cloud | <input type="text" value="Search Description"/> | <input type="text" value="Active"/> | <input type="text" value="All Permission Sets"/> |

1. Select the source as Active Directory from the list view.

A list of Active Directory groups appears in the list view.
2. Click the required group in the list view that you need to update. The Group Details page appears. The Group Details page includes three sections - Group Details, Users and Permission Set Applied.
3. **Group Details:** Name and the description fields are populated by already existing details. You cannot update group details.
4. **Custom Attributes:** Add any custom attributes from the list as required.

5. **Users:** Search the required user by entering partial or complete user name in the Search field.
 - a. To assign a user, select the user and click left single arrow icon.
 - b. To assign the complete user list, click the left double arrow icon.
 - c. To remove a user from Assigned list, click the right single arrow icon.
 - d. To remove all the users from Assigned list, click the right double arrow icon.

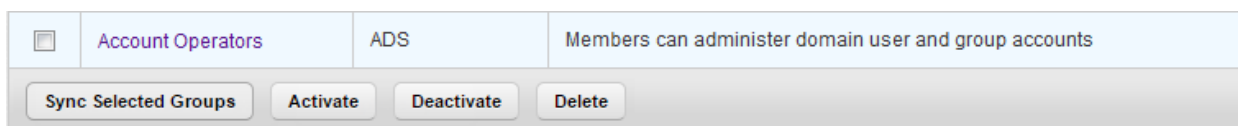


6. **Permission Set:** Select the required permission set from the **Permission Set Applied** drop-down list. All the permissions granted in the Permission Set automatically gets applied to all the Users that are part of the Group.
7. Click the **Save** button to save the details. In the message that appears, click **OK** to return to the main page. The updated Group details with applied permission set appear in the list view

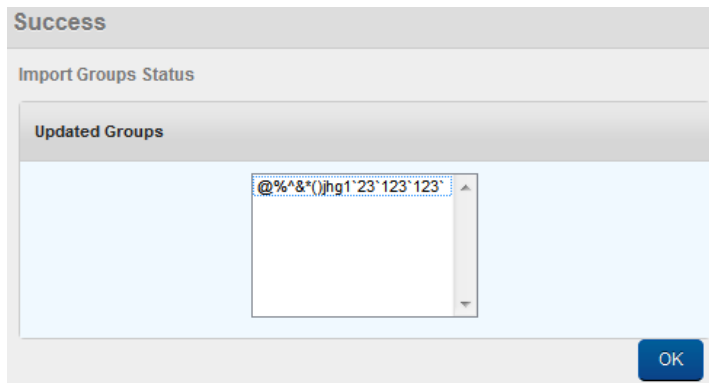
7.3.5 Sync Selected Group

The Admin can choose to synchronize an individual AD group or multiple groups. This action synchronizes all details with regards to that Group. This includes importing any new User as part of the group who are currently not part of EMM. It also includes removing any User or Users from the Group or Groups. This action is limited to AD Groups.

To Sync selected groups, follow these steps:



1. Select the required Group or Groups from the list view. The **Sync Selected Groups** button becomes active.
2. Click the **Sync Selected Groups** button. The System displays the **Success** window with a list of the updated groups.



3. Click the **OK** button to return to the main page.

7.3.6 Deactivating a Group

By default, a newly created Group appears as active in the list view under Status column. A User Group can be deactivated for various reasons. Groups on AD can only be deactivated. If apps and permissions are assigned to the users of that group, they no longer have access to the apps or permissions.

Note: You cannot deactivate the **All** group.

To deactivate a group, follow these steps:

| <input type="checkbox"/> | Group Name | Source Type | Source | Description | Status | Permission Set |
|-------------------------------------|--|---|--|---|---|--|
| | <input type="text" value="Search Groups"/> | <input type="text" value="All Source Types"/> | <input type="text" value="All Sources"/> | <input type="text" value="Search Description"/> | <input type="text" value="All Statuses"/> | <input type="text" value="All Permission Sets"/> |
| <input checked="" type="checkbox"/> | test | Local | NA | | Active | None |

1. Select the group you want to deactivate. The Deactivate button is enabled.
2. Click **Deactivate**.

The **Change Group Status** window appears asking, if the group status be deactivated.

When the Group is made inactive manually through EMM irrespective of whether the Group is an AD Group or a Local group, the following two cases are applied:

- Group not used in Targeting Apps

If the Group is not used in targeting any apps, a simple confirmation is required.

- Group used in Targeting Apps

If a Group is actively targeted for an app, the admin is informed of the same and a confirmation to delete the Group is required.

3. Click **OK** to continue.

A confirmation message about deactivated group status appears. Click **OK** to return to the main page.

The group status appears as Inactive under **Status** column in list view.

7.3.7 Deleting a Group

Admin can delete one Group or multiple groups. Before deleting a Group, the Status of the Group should be Inactive.

Note: You cannot delete the **All** group.

To delete a group,

When a Group is deleted, the Group is deleted from DB and is no longer shown in the Group list.

A group is inactivated in EMM when the a group is deactivated or deleted in Active Directory.

To delete a group, follow these steps:

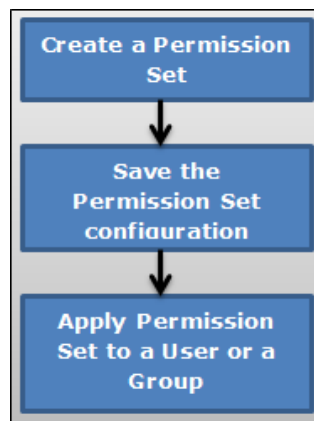
1. Ensure that the status of group is inactive.
2. Select the group you want to delete. The Delete button is enabled.
3. Click **Delete**.

The **Delete Group** window appears asking, if the group should be deleted.

4. Click **OK**.

7.4 Permission Set

A permission set is a collection of settings that give users access to various functions on a page. Permission set may be granted to any number of users. For example, in the registration page, the User is allowed to add a new Device. While users can have only one profile, they can have multiple permission sets.



The process to create a new Permission Set is as follows:

1. Create a new Permission Set.
2. Save the configuration details.
3. A new Permission is created at the end of this activity.
4. Apply Permission set to a user or a group.

From the **Access Management** tab, click **Permission Set**. The **Permission Set** page appears with the list of permissions. The list view displays a list of all the permissions along with other details. You can search the permissions based on each column.

Permission Sets [+ New Permission Set](#)

Displaying 1 - 2 of 2 - Display 10

| <input type="checkbox"/> | Permission Set | Description | Status | Last Modified On |
|--------------------------|---|---|--------------|----------------------------|
| | <input type="text" value="Search Permissions"/> | <input type="text" value="Search Description"/> | All Statuses | All |
| <input type="checkbox"/> | Admin Permissions | | Active | 12/29/2013 02:22:50 AM EST |
| <input type="checkbox"/> | Permissions Except Log Level | | Active | 12/29/2013 02:22:50 AM EST |

[Delete](#) [Previous](#) **Page {1/1}** [Next](#)

You can navigate the list view through the **Previous** and the **Next** buttons.

The Permissions list view displays the following columns:

| Columns | Description |
|------------------|--|
| Permission Set | Displays the name of the Permission Set. |
| Description | Description of the Permission Set detailing features and functionality. |
| Status | Displays the current status of the Permission set as Active or Inactive. |
| Last Modified On | Displays the date on which the Permission set was last modified. |

You can perform the following activities from the Permission Set page:

- [Creating a Permission Set](#)
- [Updating a Permission Set](#)
- [Searching for Permission Sets](#)
- [Activating/Deactivating a Permission Set](#)
- [Deleting Permission Sets](#)

7.4.1 Creating a Permission Set

Only an Admin can create a Permission Set.

To create a Permission Set, follow these steps:

Permission Sets

+ New Permission Set

1. To create a new Permission Set, click the + **New Permission Set** button next to the Permission Set label at the top of the page.

Add New Permission Set

* Required Fields

Permission Set Name *

Description

Save Save & Edit Cancel

Add New Permission Set window appears.

2. Enter details for the following fields:
 - a. **Permission Set Name:** Enter an appropriate name for the Permission Set. You cannot create permission set names with Special characters such as `/\ [] ; | = , + * ? < > @ "`
 - b. **Description:** Enter an appropriate description of the Permission Set that clearly indicates its objective.
3. Click the **Save** button to save the details. In the confirmation message that appears, click **OK** to continue.

The newly added permission set is displayed in the list view. By default, the newly created Permission Set appears as active in the list view under Status column.

4. Click the **Save and Edit** button to update the Permission Set. This action opens the Permission Set details page. You can update the permission sets by following the next procedure.

7.4.2 Adding/Updating a Permission Set

You add permissions to provide App Management page permissions to a user. By providing page level permissions, the User has permissions to view the page and perform all actions on the page.

To add/update details of a permission set, follow these steps:

1. Click the required permission set in the list view that you need to update.

The **Permission Set Details** page appears.

Permission Set Details

[Permission Sets](#) > Doc

The screenshot shows the 'Permission Set Details' page with the 'Limited Access' tab selected. The page has a breadcrumb trail 'Permission Sets > Doc'. Below the breadcrumb, there are five tabs: 'Limited Access', 'Common Settings', 'App Management', 'Device Management', and 'Content Management'. The 'Limited Access' tab is active. Below the tabs, there is a form with a label 'Limit Access' and two radio buttons: 'Yes' and 'No'. The 'No' radio button is selected. At the bottom of the form, there are two buttons: 'Save' and 'Cancel'.

The Permission Set Details page includes the following tabs:

- Description
- Limited Access
- Common Settings
- App Management

- Device Management
 - Content Management
2. **Description:** Displays a brief description about the Permission set (entered by a user).
 3. **Limited Access To Device List:** By default, the Limit Access option is set to **No**. Select **Yes** to set limited access definition. By choosing Yes, you can create a permission set that grants limited access to users, groups, devices, device sets, folders, and targeting. Assigning the same to a user makes that user a limited administrator.

For more details, refer to [Limited Access to Users, Groups and Device List](#).

4. Common Settings

- **Dashboard:** When **Yes** is selected, a user views the dashboard of EMM. If **No** is selected, the link for Dashboard is not visible in the left navigation panel.
- **Access Management Page Permissions:** By choosing yes against each option, an administrator can grant a user access to the following pages in the access management section:
 - **Reports:** The administrator views and accesses the Reports page from the left navigation panel. This is a prerequisite to view report details and perform any action on reports.
 - **Users:** The administrator views and accesses the Users page from the left navigation panel. This is a prerequisite to view user details and perform any action on users.
 - **User Details:** The administrator views details of Users. This is a prerequisite to update user details, modify groups associated with the user.
 - **Groups:** The administrator views and access the Groups list page from the left navigation panel. This is a prerequisite to view Group Details and perform any action on Groups.

- **Group Details:** The administrator views details of the Groups. This is a prerequisite to update group details or modify Users associated with Groups.
- **Permissions Set:** The administrator views and access the list of Permission Sets. This is a prerequisite to view Permission Set Details and perform any actions on Permission Sets.
- **Permission Set Details:** The administrator views details of Permission Sets. This is a prerequisite to update permissions and define limited access.
- **Access Management Action Permissions:** By setting any of the following actions to yes, an administrator allows a user to perform that action.
 - **Reports:**
 - **Device Inventory Report:** Set to **Yes** to user to create a device inventory report.
 - **App Inventory Report:** Set to **Yes** to create an app inventory report.
 - **Content Download History Report:** Set to **Yes** to create a content download history report.
 - **Compliance Actions Report:** Set to **Yes** to create a compliance actions report.
 - **App Usage Report:** Set to **Yes** to create an app usage report.
 - **Call Usage Report:** Set to **Yes** to create a call usage report.
 - **SMS Usage Report:** Set to **Yes** to create an SMS usage report.
 - **App Network Usage Report:** Set to **Yes** to create an app network usage report.
 - **User Device Report:** Set to **Yes** to create a user device report.
 - **App Rating Report:** Set to **Yes** to create an app ratings report.

- **Users:**
 - **Create User:** Set to **Yes** to create local users in EMM.
 - **Delete User:** Set to **Yes** to delete users (both local and active directory) from EMM.
 - **Update User Details:** Set to **Yes** to modify user details. This is a prerequisite to Add/Remove Groups to/from User.
 - **Import User from AD:** Set to **Yes** to import new users from Active Directory into EMM.
 - **Add/Remove Groups to/from User:** Set to **Yes** to associate another user with groups or remove such associations. For this action the Add/Remove Users to/from Group also must be set to **Yes**.
 - **Apply Permission Set to Users:** Set to **Yes** to apply and modify permission sets applied to other users.
 - **Define Permissions:** Enter permission sets applicable on the user.
 - **Assign Custom Attributes to Users:** Set to **Yes** to assign custom attributes to users.
 - **Sync Selected Users:** Set to **Yes** to begin an ad hoc sync with Active Directory for the selected users.
 - **Reset Password:** Set to **Yes** to reset the password for local users only.
- **Groups:**
 - **Create Group:** Set to **Yes** to allow a user to create local groups.
 - **Delete Group:** Set to **Yes** to allow a user to delete local and Active Directory groups from EMM.

- **Update Group Details:** Set to **Yes** to allow a user to update group details. This is a prerequisite to Add/Remove users to/from a group.
- **Import Group from AD:** Set to **Yes** to allow a user to import new groups from Active Directory to EMM.
- **Add/Remove Users to/from Group:** Set to **Yes** to allow a user to modify the users associated with groups. For this action, the Add/Remove Groups to/from User also must be set to **Yes**.
- **Apply Permission Set to Groups:** Set to **Yes** to allow a user to add or modify permission sets assigned to Groups.
- **Define Permissions:** Enter permission sets applicable on the user.
- **Assign Custom Attributes to Groups:** Set to **Yes** to assign custom attributes to groups.
- **Sync Selected Groups:** Set to **Yes** to initiate an ad hoc sync with active directory for the selected groups.
- **Permission Sets:**
 - **Create Permission Set:** Set to **Yes** to allow a user to create permission sets.
 - **Delete Permission Sets:** Set to **Yes** to allow a user to delete permission sets.
 - **Update Permission Set Details:** Set to **Yes** to allow a user to update Permission Set Details. This is a prerequisite for Limit Access.
 - **Limit Access:** Set to **Yes** to allow a user to limit Permission Set Details.
- **Settings Page Permissions:** By checking yes against each of the following pages, you grant a user access to those pages.

- **Content Settings**
 - **Content Settings:** You can view and access the Content Settings page from the left navigation panel. You must have this permission to enable any other pages and actions under Content Settings Actions.
 - **Usage Settings:** Set to **Yes** to see the Usage Settings for Content Management. This is a pre-requisite to the action - Update Usage Settings.
 - **Message Templates:** Set to **Yes** to view all the automated message templates relevant to Content Management. This is a pre-requisite to the action - Edit Message Template.
 - **Error Messages:** Set to **Yes** to view all the Policy Error messages that Users would see on their devices if they violated any policies. This is a pre-requisite to the action - Update Error Messages.

- **Device Settings:**
 - **Device Settings:** Set to **Yes** to view and access the Device Settings page from the left navigation panel. This is a pre-requisite to being able to enable any other pages and actions under Device Settings Actions.
 - **Usage Settings:** Set to **Yes** to see the Usage Settings for Device Management. To update this, you must have the permission to Update Device Settings.
 - **Message Templates:** Set to **Yes** to view all the automated message templates relevant to Device Management. This is a pre-requisite to the actions - Add Message Templates and Delete Message Templates.

- **Terms and Conditions:** Set to **Yes** to view the Terms and Conditions of using EMM as shown to Users during enrollment. To update this, you must have the permission to Update Device Settings.
- **Communication Configuration:** Set to **Yes** to view the certificate details and communication server details for Device Management activities. To update this, you must have the permission to Update Device Settings.
- **App Settings:**
 - **App Settings:** Set to **Yes** to view and access the Application Settings page from the left navigation panel. This is a pre-requisite to being able to enable any other pages and actions under App Settings Actions.
 - **Usage Settings:** Set to **Yes** to see the Usage Settings for Device Management. This is a pre-requisite to the action - Update App Settings - Usage Settings.
 - **Policy Error Messages:** Set to **Yes** to view all the Policy Error messages that Users would see on their devices if they violated any policies. This is a pre-requisite to the action - Update App Settings - Policy Error Messages.
 - **Encryption Key:** Set to **Yes** to view all the encryption seeds generated. This is a pre-requisite to the action - Create Encryption Key.
 - **Certificates:** Set to **Yes** to see all the app management related certificates uploaded to EMM for each of the different platforms supported. This is a pre-requisite to the action - Update App Settings - Certificates.

- **Message Templates:** Set to **Yes** to see all the message templates for App Management. This is a pre-requisite to the action - Edit Message Templates.
- **VPP Apps:** Set to **Yes** to see Volume Purchase Apps Settings. This is a pre-requisite for the actions - Update App Settings - VPP Apps and Sync VPP Apps.
- **Directory Settings:**
 - **Directory Settings:** Set to **Yes** to view and access the Directory Settings page from the left navigation panel. This is a pre-requisite to view the tabs below and actions under Directory Settings actions.
 - **Directory Details - Definition:** Set to **Yes** to see the Directory Details definition.
 - **Directory Details - Synchronization Schedule:** Set to **Yes** to see the Synchronization Schedule for each directory. This is a pre-requisite to the action - Complete Sync.
- **Enrollment Mode**
 - **Enrollment Mode:** Configure to **Yes** to enable enrollment mode features for a limited administrator. By default, this is configured to **No**.
- **Geo & Time Fences:**
 - **Geo and Time Fences:** Set to **Yes** to view and access the Geo and Time Fences page from the left navigation panel. This is a pre-requisite to view the tabs (Geo-fences and time Fences) and actions under Geo and Time Fences actions.
 - **Geo-fences:** Set to **Yes** to view the list of Geo-fences in the system. This is a pre-requisite to being able to view the page Geo-fence details and the actions - Add Geo-fences and Delete Geo-fences.

- **Geo-fence details:** Set to **Yes** to view the details of each Geo-fence. This is a pre-requisite for the action - Update Geo-fence details.
- **Time Fences:** Set to **Yes** to view the list of Time Fences in the system. This is a pre-requisite to being able to view the page Time Fence details and the actions - Add Time Fences and Delete Time Fences.
- **Time Fence details:** Set to **Yes** to view the details of each Time Fence. This is a pre-requisite for the action - Update Time Fence details.
- **Branding:**
 - **Branding:** Set to **Yes** to view and access the Branding page from the left navigation panel. This is a pre-requisite to being able to view the tabs listed below and actions under Branding actions.
 - **Web Consoles:** Set to **Yes** to view all the branding images provided for Web Consoles Logo and Favicon.
 - **Enterprise Store Download:** Set to **Yes** to view all the branding images for the enterprise store Download page (across platforms).
 - **Enterprise Store Login:** Set to **Yes** to view all the branding images for the enterprise store Login page (across platforms).
 - **Splash Screen:** Set to **Yes** to view all the branding images for the Splash Screen as enterprise store loads (across platforms).
 - **Enterprise Store Springboard Icons:** Set to **Yes** to view all the branding images for the Springboard icons for enterprise store (across platforms).

- **Enterprise Resources:**
 - **Enterprise Resources:** Set to **Yes** to view and access the Enterprise Resources page from the left navigation panel. This is a pre-requisite to view the tabs for Wi-Fi, VPN, Certificates, Airplay and Airprint lists. It is also a pre-requisite for all actions under Enterprise Resources.
 - **Wi-Fi List:** Set to **Yes** to see the list of Wi-Fi configurations created in EMM. This is a pre-requisite for the Wi-Fi Details page and the actions - Add Wi-Fi, Delete Wi-Fi and Update Wi-Fi Details.
 - **Wi-Fi Details:** Set to **Yes** to see details of the Wi-Fi configurations created in EMM. This is a pre-requisite for the action - Update Wi-Fi Details.
 - **VPN List:** Set to **Yes** to see the list of VPN configurations created in EMM. This is a pre-requisite for the VPN Details page and the actions - Add VPN, Delete VPN and Update VPN Details.
 - **VPN Details:** Set to **Yes** to see details of the VPN configurations created in EMM. This is a pre-requisite for the action - Update VPN Details.
 - **Certificates List:** Set to **Yes** to see the list of Certificates created in EMM (for distribution). This is a pre-requisite for Certificate Details page and the actions - Add Certificates, Delete Certificates and Update Certificate Details.
 - **Certificate Details:** Set to **Yes** to see the details of certificates listed. This is a pre-requisite for the action - Update Certificate details.
 - **AirPlay Settings:** Set to **Yes** to see the list of AirPlay Settings created. This is a pre-requisite to the actions - Add AirPlay Configuration, Delete Airplay Configuration and Update AirPlay Details.

- **AirPrint Settings:** Set to **Yes** to see the list of AirPrint Settings created. This is a pre-requisite to the actions - Add AirPrint Configuration, Delete AirPrint Configuration and Update AirPrint Details.
- **Admin Email Settings:** These Settings are required to send emails to Users. Several actions and policies are dependent on this setting.
 - **Admin Email Settings:** Set to **Yes** to view and access the Admin Email Settings page from the left navigation panel. This is a pre-requisite to the action under Admin Email Settings.
- **Custom Attributes:**
 - **Custom Attributes Set List:** Set to **Yes** to view custom attributes set list.
 - **Custom Attributes Details:** Set to **Yes** to view custom attributes set details.
- **Exchange Settings**
 - **Exchange Settings:** Set to **Yes** to view and access the Exchange Services page from the left navigation panel. This is a pre-requisite to the actions under Exchange Services.
- **Event Log**
 - **Event Log:** Set to **Yes** to view and access the Event Log page from the left navigation panel.
- **System Status**
 - **System Status:** Set to **Yes** to view and access the System Status page from the left navigation panel. This is a pre-requisite to perform actions under System Status.

- **Health Check:** Set to **Yes** to view the Health Check parameters for EMM. You can get the latest status of any of the parameters individually or all services at once.
- **Job Monitor:** Set to **Yes** to view the jobs running on EMM. This is a pre-requisite to the actions - Start Job and Stop Job.
- **Log Levels:** Set to **Yes** to view all the Log Levels.
- **Settings Action Permissions**
 - **Device Settings**
 - **Add Message Templates:** Set to **Yes** to add new message templates or edit existing ones. These will show up when any admin user wants to send messages to devices or device sets.
 - **Delete Message Templates:** Set to **Yes** to delete message templates you created. You cannot delete existing message templates as they are required for the functioning of EMM.
 - **Update Device Settings:** Set to **Yes** to update Device Settings. If none of the Device Settings tabs are accessible, this is set to No and is inactive.
 - **App Settings**
 - **Create Encryption Key:** Set to **Yes** to create encryption keys which are used for encrypting app data.
 - **Sync VPP Apps:** Set to **Yes** to sync VPP apps.
 - **Edit Message Template:** Set to **Yes** to edit and modify any of the App Management message templates. None of the message templates can be deleted. If set to **No**, you can view the templates but not edit them.

- **Update App Settings - Certificates:** Set to **Yes** to edit and modify any of the certificates uploaded. If set to **No**, you can only view the tab.
- **Update App Settings - Usage Settings:** Set to **Yes** to edit and modify the Usage Settings for App Management. If set to **No**, you can only view the tab.
- **Update App Settings - Policy Error Messages:** Set to **Yes** to edit and modify the Policy Error Messages. If set to **No**, you can only view the tab.
- **Update App Settings - VPP Apps:** Set to **Yes** to edit and modify the VPP App Settings. If set to **No**, you can only view the tab.
- **Directory Settings**
 - **Add Directory:** Set to **Yes** to add a new directory.
 - **Delete Directory:** Set to **Yes** to delete any of the directories.
 - **Update Directory Details:** Set to **Yes** to edit and update Directory Details and Synchronization Schedules. If neither of the tabs Directory Details - Definition and Synchronization Schedule are allowed, then this action will be set to **No** and will not be active.
 - **Complete Sync:** If set to **Yes**, based on the Synchronization type, you can either sync imported users and groups or sync all users and groups from the active directory. If neither are allowed, you can only view the page.
- **Custom Attributes**
 - **Create Attributes Set:** Setting this to **Yes** will allow a user to create a custom attribute set.
 - **Copy Attributes Set:** Setting this to **Yes** will allow a user to copy an existing custom attribute set.

- **Delete Attributes Set:** Setting this to **Yes** will allow a user to delete an existing custom attribute set.
- **Update Attributes Set details:** Setting this to **Yes** will allow a user to update an existing custom attribute set.
- **Exchange Settings**
 - **Update Exchange Settings:** Set to **Yes** to update the Exchange Services configuration and the Mail Clients which are Whitelisted or Blacklisted.
 - **Add Agent (Mail Client):** Set to **Yes** to add new Mail Clients to the master list.
- **Content Settings:**
 - **Update Content Usage Settings:** Set to **Yes** to can edit and modify the Usage Settings.
 - **Edit Message Template:** Set to **Yes** to edit the message templates.
 - **Update Content Policy Error Messages:** Set to **Yes** to edit and modify the Policy Error Messages.
- **Branding:**
 - **Update Branding Settings:** Set to **Yes** to edit and modify the icon images in any of the tabs.
- **Admin Email Settings:**
 - **Update Admin Email Settings:** Set to **Yes** to edit and modify Admin Email Settings.
- **System Status:**
 - **Start Job:** Set to **Yes** to start the job if it is stopped.
 - **Stop Job:** Set to **Yes** to stop a job that is running.

- **Geo and Time Fences:**
 - **Add Geo-fences:** Set to **Yes** to add new geo-fences.
 - **Delete Geo-fences:** Set to **Yes** to delete existing geo-fences.
 - **Update Geo-fence details:** Set to **Yes** to update the geo-fence details.
 - **Add Time Fences:** Set to **Yes** to add time fences.
 - **Delete Time Fences:** Set to **Yes** to delete time fences.
 - **Update Time Fence details:** Set to **Yes** to update time fence details.
- **Enterprise Resources:**
 - **Add Wi-Fi:** Set to **Yes** to add new Wi-Fi configurations.
 - **Delete Wi-Fi:** Set to **Yes** to delete Wi-Fi configurations.
 - **Update Wi-Fi Details:** Set to **Yes** to update Wi-Fi Details.
 - **Add VPN:** Set to **Yes** to add new VPN connections.
 - **Delete VPN:** Set to **Yes** to delete existing VPN connections.
 - **Update VPN Details:** Set to **Yes** to update VPN details.
 - **Add Certificates:** Set to **Yes** to add new certificates.
 - **Delete Certificates:** Set to **Yes** to delete existing certificates.
 - **Update Certificate Details:** Set to **Yes** to update certificate details.
 - **Add AirPlay Configuration:** Set to **Yes** to add new AirPlay configurations.
 - **Delete AirPlay Configuration:** Set to **Yes** to delete existing AirPlay configurations.

- **Update AirPlay Details:** Set to **Yes** to edit AirPlay details.
- **Add AirPrint Configuration:** Set to **Yes** to add new AirPrint configurations.
- **Delete AirPrint Configuration:** Set to **Yes** to delete existing AirPrint configurations.
- **Update AirPrint Details:** Set to **Yes** to edit AirPrint details.

5. App Management:

In this section, if none of the permissions are set to **Yes**, this section does not display for the user.

- **App Management Page Permissions**
 - **Enterprise Apps:** Set to **Yes** to view and access the Enterprise Apps page from the left navigation panel.
 - **App Details:** Set to **Yes** to able to view the App Details page. This is a pre-requisite for the actions - Upgrade App, Add a Platform and Update App Details.
 - **App Policies:** Set to **Yes** to able to view the link and access the App Policies page from the left navigation panel.
 - **App Policy Details:** Set to **Yes** to able to view the App Policy Details page. This is a pre-requisite for the action - Update App Policy Details.
 - **Categories:** Set to **Yes** to view the link and access the Categories page from the left navigation panel. This is a pre-requisite for the action under Categories.
 - **VPP Apps:** Set to **Yes** to view the link and access the VPP Apps page from the left navigation panel. This is a pre-requisite for the tabs below (Purchased App List, Invited Users) and all the actions under VPP Apps.

- **Purchased App List:** Set to **Yes** to view the Purchased App List tab and its contents. This is a pre-requisite to the actions - Sync Now, Target Users and Recall Licenses.
- **Invited Users:** Set to **Yes** to view the Invited Users tab and its contents. This is a pre-requisite to the actions - Retire Users, Send Invite Again.
- **App Management Action Permissions**
 - **Enterprise Apps**
 - **Add an App:** Set to **Yes** to add a new Enterprise App.
 - **Upgrade App:** Set to **Yes** to upgrade the version of the app.
 - **Add a Platform:** Set to **Yes** to add a new platform for the app.
 - **Update App Details:** Set to **Yes** to update app details for the apps you own and save the same.
 - **Target App(s):** Set to **Yes** to target the app to Users and Groups. From the App Details page, you must also have the permission to update app details to save changes to targeting.
 - **Own App:** Set to **Yes** to own the app if it is owned by someone else so that you can modify the same.
 - **Approve App:** Set to **Yes** to approve an app.
 - **Publish/Unpublish App:** Set to **Yes** to Publish and Unpublish the apps.
 - **Wrapping/Signing:** Set to **Yes** to invoke a Wrap or sign action on an app where it has failed.
 - **Delete App:** Set to **Yes** to delete apps.
 - **Assign Custom Attributes to Apps:** Setting this to **Yes** will allow a user to assign custom attributes to an enterprise app.

- **Update App Licenses:** Setting this to **Yes** will allow a user to update app licenses for an enterprise app.
- **Recall App Licenses:** Setting this to **Yes** will allow a user to recall app licenses for an enterprise app.
- **App Policies:**
 - **Create a Policy:** Set to **Yes** to create an app policy.
 - **Own Policy:** Set to **Yes** to own app policies that are owned by someone else.
 - **Activate Policy:** Set to **Yes** to activate policy.
 - **Publish/Unpublish Policy:** Set to **Yes** to publish or un-publish policies.
 - **Delete Policy:** Set to **Yes** to delete app policies.
 - **Update Policy Details:** Set to **Yes** to update and save app policy details for the policies you own.
- **Categories:**
 - **Create Category:** Set to **Yes** to create a new category.
 - **Delete Category:** Set to **Yes** to delete categories.
 - **Edit Category:** Set to **Yes** to edit categories.
- **VPP Apps:**
 - **Sync Now:** Set to **Yes** to Sync the list VPP Apps available with the Apple Server.
 - **Target Users:** Set to **Yes** to target the VPP Apps to Users and Groups.
 - **Recall Licenses:** Set to **Yes** to Recall Licenses from Users to whom they are issued.

- **Retire Users:** Set to **Yes** to Retire Users from the Volume Purchase Program (VPP).
- **Send Invite Again:** Set to **Yes** to send an invite again to users that have not joined the VPP.

6. **Device Management Page Permissions** If none of the page permissions are **Yes** in this section, the section does not display for the user. Set the permission details for the Device Management page for the following fields:

- **Device Management Page Permissions:**
 - **Device List/Details**
 - **Devices:** Set to **Yes** to view and access the Devices page from the left navigation panel. This is a pre-requisite to view Device Details and perform any action under Devices.
 - **Device Details:** Set to **Yes** to view Device Details. This is a pre-requisite to all tabs in Device Details (Overview, Locate, Messages, App Monitor, Asset Properties, Services and EMM Info) and all actions under Devices except View policies applied to a device and Delete Device.
 - **Overview:** Set to **Yes** to view the overview details of each device. This is a pre-requisite to the action - Remove All Certificates.
 - **Locate:** Set to **Yes** to view the current and last few locations of the device.
 - **Messages:** Set to **Yes** to all the messages sent to the device. This is a pre-requisite for the action - Send Message.
 - **App Monitor:** Set to **Yes** to view all the apps present on each device. This is a pre-requisite to the action - Delete App.
 - **Asset Properties:** Set to **Yes** to view all the Asset Property details of the device.
 - **Services:** Set to **Yes** to view all the services running on Windows 8.1 devices.

- **EMM Info:** Set to **Yes** to view all the information about the EMM as on device. This is a pre-requisite for the Purge action.
- **Device Policy:**
 - **Device Policies:** Set to **Yes** to view and access the Device Policies page from the left navigation panel. This is a pre-requisite to view Device Policy Details and perform any action under Device Policies.
 - **Device Policy Details:** Set to **Yes** to view Device Police Details. This is a pre-requisite for the actions Update Policy Details and Change Priority.
- **Device Set**
 - **Device Set:** Set to **Yes** to view and access the Device Set page from the left navigation panel. This is a pre-requisite to view Device Set Details and perform any action under Device Set.
 - **Device Set Details:** Set to **Yes** to view Device Set Details. This is a pre-requisite for the tabs below (Conditions, Current Devices, Messages) and the actions - Update Device Set Details and Apply Policies to Device Set.
 - **Conditions:** Set to **Yes** to view the Conditions tab.
 - **Current Devices:** Set to **Yes** to view the Current Devices tab.
 - **Messages:** Set to **Yes** to view the Messages tab.
- **Enrollment**
 - **Enrollment:** Set to **Yes** to view and access the Device Enrollment page from the left navigation panel. This is a pre-requisite to perform any action under Device Enrollment.
- **Device Management Action Permission**
 - **Device List/Details**
 - **View Policies applied on Device:** Set to **Yes** to view Policies applied to devices from the Devices page as well as the details page.

- **Force Check-in:** Set to **Yes** to force the device to connect with the EMM Server and respond.
- **Lock Device:** Set to **Yes** to remotely lock the device.
- **Reset/Clear Password:** Set to **Yes** to reset the device's passcode.
- **Wipe Wizard:** Set to **Yes** to either Enterprise Wipe or completely wipe the device.
- **Block/Unblock Email:** Set to **Yes** to Block/Unblock Email for the device.
- **Remove App Data:** Set to **Yes** to remove app data for all enterprise apps.
- **Resume Device:** Set to **Yes** to resume suspended devices.
- **Start/Stop Mirroring:** Set to **Yes** to start and stop mirroring for iOS 7+ devices.
- **Power Off Device:** Set to **Yes** to remotely power off SAFE devices.
- **Lock SIM:** Set to **Yes** to lock a SIM to a SAFE device.
- **Remove All Certificates:** Set to **Yes** to remove all certificates on the device.
- **Update Device Details:** Set to **Yes** to update and save device details.
- **Assign Custom Attributes to Devices:** Setting this to Yes will allow a user to assign custom attributes on a device.
- **Send Messages:** Set to **Yes** to send messages to devices.
- **Delete Apps:** Set to **Yes** to delete apps on devices from App Monitor.
- **Delete Device:** Set to **Yes** to delete a device from the Devices list.

- **Enrollment:**
 - **Add a Device:** Set to **Yes** to add a single device to be enrolled.
 - **Bulk Enroll:** Set to **Yes** to invoke the bulk enroll command.
- **Device Set:**
 - **Create Device Set:** Set to **Yes** to create device sets.
 - **Approve Device Set:** Set to **Yes** to change device sets state.
 - **Publish/Unpublish Device Set:** Set to **Yes** to change device set status.
 - **Copy Device Set:** Set to **Yes** to copy the definition of a device set to a new one.
 - **Delete Device Set:** Set to **Yes** to delete device sets.
 - **Apply Policies to Device Set:** Set to **Yes** to apply policies to device sets.
 - **Update Device Set Details:** Set to **Yes** to update and save device set details. If not, all device set tabs are read only.
- **Device Policy:**
 - **Create Policy:** Set to **Yes** to create device policies.
 - **Activate Policy:** Set to **Yes** to modify the state of device policies.
 - **Publish/Unpublish Policy:** Set to **Yes** to modify the status of device policies.
 - **Copy Policy:** Set to **Yes** to copy the definition of a device policy to a new one.
 - **Change Priority:** Set to **Yes** to change the priority of a policy.
 - **Delete Policy:** Set to **Yes** to delete device policies.

- **Update Policy Details:** Set to **Yes** to update and save device policy details. If not all policy tabs are read-only.

7. Content Management:

• Content Management Page Permissions

- **Files:** Set to **Yes** to view and access the link on the left navigation panel to the Files page. This is a pre-requisite for File Details and all actions under Files.
- **Files Details:** Set to **Yes** to view File Details. This is a pre-requisite to the tabs below (Description, Current Version, Past Version) and the actions - Update File Details, Rename File, Make File as Current Version, Download File Version, Update File Version.
- **File Details - Description Tab:** Set to **Yes** to view the Description tab.
- **File Details - Current Version Tab:** Set to **Yes** to view the Current Version tab
- **File Details - Past Version Tab:** Set to **Yes** to view the past version tab. This a pre-requisite to Make File as Current Version.
- **Folders:** Set to **Yes** to view and access the link on the left navigation panel to the Folders page. This is a pre-requisite for Folder Details and all actions under Folders.
- **Folder Details:** Set to **Yes** to view Folder Details. This is a pre-requisite for the tabs below (Details, Content, Targeting) and the actions - Copy From, Move From, Target Folders, Update Folder Details, Rename Folder, Add New File and Add New Folder.
- **Folder Details - Details Tab:** Set to **Yes** to view the Details tab.
- **Folder Details - Content Tab:** Set to **Yes** to view the Content tab.
- **Folder Details - Targeting Tab:** Set to **Yes** to view the targeting tab. This is a pre-requisite to the action - Target Folders.

- **Content Policies:** Set to **Yes** to view and access the link on the left navigation panel to the Content Policies page. This is a pre-requisite for Content Policy Details and all actions under Content Policies.
- **Content Policies Details:** Set to **Yes** to view content policy details. This is a pre-requisite for the actions - Update Policy.
- **Content Management Action Permissions**
 - **File**
 - **Add New File:** Set to **Yes** to add new files to EMM from either Files or Folder Details. If no, you cannot add new files from either location.
 - **Delete File:** Set to **Yes** to delete files from EMM.
 - **Copy to:** Set to **Yes** to copy files to destination folders.
 - **Move to:** Set to **Yes** to move files to destination folders.
 - **Update File Details:** Set to **Yes** to modify file details and save the same.
 - **Rename File:** Set to **Yes** to rename the file.
 - **Make File as Current Version:** Set to **Yes** to select an older version of the file and make it the current version.
 - **Download File Version:** Set to **Yes** to be allowed to download the current version and older versions of a file.
 - **Update File Version:** Set to **Yes** to update the file version.
 - **Folders:**
 - **Add New Folder:** Set to **Yes** to add new folders to EMM from the Folders list page and from Folder details.
 - **Delete Folder:** Set to **Yes** to delete folders.
 - **Copy To:** Set to **Yes** to copy the folder to a destination folder.

- **Move To:** Set to **Yes** to move the folder to a destination folder.
- **Copy From:** Set to **Yes** to copy files or folders from a source folder.
- **Move From:** Set to **Yes** to move files or folders from a source folder.
- **Update Folder Details:** Set to **Yes** to modify and save folder details.
- **Target Folders:** Set to **Yes** to target folders to users and groups.
- **Create New File:** Set to **Yes** to add new files to folders.
- **Create New Folder:** Set to **Yes** to create new folders within folders.
- **Rename Folder:** Set to **Yes** to rename folders.
- **Content Policies:**
 - **Add Policy:** Set to **Yes** to add new content policies to EMM.
 - **Delete Policy:** Set to **Yes** to delete content policies.
 - **Activate Policy:** Set to **Yes** to modify the state of content policies.
 - **Publish/Unpublish Policy:** Set to **Yes** to modify the status of content policies.
 - **Copy Policy:** Set to **Yes** to copy the content of the policy to a new policy.
 - **Update Policy:** Set to **Yes** to modify and save policies.
- **Content Repository:**
 - **Add Repository:** Set to **Yes** to enable the user to add a new repository.
 - **Edit Repository:** Set to **Yes** to enable the user to edit an existing repository.
 - **Delete Repository:** Set to **Yes** to enable the user to delete an existing repository.

8. Click the **Save** button. In the message that appears, click **OK** to return to the main page. The updated permission set details appear in the list view.

7.4.3 Searching for Permission Sets

You can search for a desired permission set through the available search filters. You can apply a single or a combination of search filters to define the search criteria and get the refined outcome.

| Permission Set | Description | Status | Last Modified On |
|---|---|--------------|----------------------------|
| <input type="text" value="Search Permissions"/> | <input type="text" value="Search Description"/> | All Statuses | All |
| <input type="checkbox"/> Sample Permission Set | Sample Permission Set | Active | 12/29/2013 08:23:51 AM EST |
| <input type="checkbox"/> Admin Permissions | | Active | 12/29/2013 02:22:50 AM EST |

1. Enter or select details for following search filters:
 - a. **Permission Set:** Enter partial or complete name of the permission set in the **Search Permission** field.
 - b. **Description:** Enter partial or complete description of the permission set in the **Search Description** field.
 - c. **Status:** Select the required status from the drop-down list.
 - d. **Last Modified on:** Select the required date on which the permission set was last modified.
2. The list view is updated with respective permission set details, as per the search criteria. By default, the list view displays ten permission sets according to Display settings that you can modify through the **Display** drop-down list. You can also scroll the list view through **Previous** and the **Next** button.

7.4.4 Activating/Deactivating Permission Sets

If you do not want to apply a permission set to a User or a Group temporarily, you can deactivate it. Still the deactivated permission remains as applied on the respective user and groups but no permissions can be used as the permission set is in deactivated mode.

To deactivate a Permission Set, follow these steps:

| Permission Set | Description | Status | Last Modified On |
|--|---|----------------------|----------------------------|
| <input type="text" value="Search Permissions"/> | <input type="text" value="Search Description"/> | All Statuses | All |
| <input type="checkbox"/> Sample Permission Set | Sample Permission Set | Active Deactivate | 12/29/2013 08:23:51 AM EST |

1. Select the Status as **Deactivate** for the required Permission Set in the list view.

The **Change Permission Status** window appears asking, if the permission set status be deactivated. Click **Ok** to continue.

2. The System displays the confirmation message. Click **Ok** to return to the main page.

To activate a Permission Set, follow these steps:

1. Select the Status as **Active** for the required Permission Set in the list view.

The **Change Permission Status** window appears asking, if the permission set status be activated.

2. Click **Ok** to continue.

The System displays the confirmation message.

3. Click **OK** to return to the main page.

7.4.5 Deleting Permission Sets

If a permission set is no longer required for a user or group, you can delete the permission set. Before the permission set is deleted, change the status of the permission set to a deactive state.

When a permission set is deleted, the status of its associated device set changes to unpublished. The device set state changes to draft.

To delete a permission set, follow these steps:

| <input type="checkbox"/> | Permission Set | Description | Status | Last Modified On |
|-------------------------------------|---|---|----------------|----------------------------|
| | <input type="text" value="Search Permissions"/> | <input type="text" value="Search Description"/> | All Statuses ▾ | All ▾ |
| <input checked="" type="checkbox"/> | Sample Permission Set | Sample Permission Set | Inactive ▾ | 12/29/2013 09:42:18 AM EST |
| <input type="checkbox"/> | Admin Permissions | | Active ▾ | 12/29/2013 02:22:50 AM EST |
| <input type="checkbox"/> | Permissions Except Log Level | | Active ▾ | 12/29/2013 02:22:50 AM EST |

Page {1/1}

1. Click the check box, next to the permission set that you want to deactivate.

The **Delete** button becomes active.

2. Click the **Delete** button. In the confirmation dialog that appears, click **Yes** to proceed.

The system displays the confirmation message.

3. Click **Ok** to return to the main page.

The deleted permission set is removed from the list view.

7.4.6 Resolving Permissions

Different user permissions may be applied to a designated user's individual account and a group account that includes the user. However, the user receives all the permissions that are granted to either the individual account or the group account.

For example:

- User John is granted the permission to Apps, Policies, and Categories.
- Group A is granted Permissions for Users, Groups, Approve Apps, and Publish Apps.
- Group B is granted permission for Users, Groups, Dashboards, and MAM Settings.

If User John is part of both Group A and B, then he receives the following permissions:

- **Page Level Permissions**

- Apps
- Policies
- Categories
- Users and Groups
- Dashboards
- MAM Settings

- **Action Level Permissions**

- Approve Apps
- Publish Apps

8. Device Registration

Important:

Supported Devices:

Android: Kony Management (EMM) supports Android devices that are on OS version 4.4.x (KITKAT) and later.

iOS: Kony Management (EMM) supports Apple devices that are on iOS version 9.0 and later.

The only devices that can be registered are iOS and Android devices.

The process of registration is very simple. A User must be created in EMM or imported from an AD. The User must access the enterprise store download URL (communicated to them through a mail invitation or otherwise). The User downloads enterprise store, installs the same - logs into it and agrees to the terms and conditions. This completes the registration of the device with the User. The process is the same across iOS and Android devices.

Important: On your Android devices, ensure that the Developer Options feature is not enabled. If the Developer Options feature is enabled, your device registration may fail.

8.1 Device Registration- Post Confirmation Details (Admin)

The next steps after receiving an email with a URL and details of how to register with EMM Server are as follows

- [Enterprise Store Download](#)
- [Authentication](#)
- [Terms Acceptance](#)
- [Profile Download](#)

8.1.1 Enterprise Store Download

1. The Device User (Employee) accesses the mentioned URL and downloads the device agent app.
2. The Device User installs the app.

You can download an Enterprise store, in two ways of authentication.

- Using Kony Management suite user login credentials
- Using Kony Fabric Identity Service OAuth 2.0 user login credentials.

8.1.2 Authentication

1. The Device User provides authentication details in the email message, through providing Company Name, AD User Name and Password.
2. Submitted details are sent to the Server with device information.
3. The EMM Server ensures that the device is not registered, not associated with any other user. Once this is established, the server signals the agent to proceed with the registration.

4. If Verification fails, device user receives a message. Device goes into the status based on type of verification failure.

8.1.3 Terms Acceptance

1. Once the authentication and verification is successful, the device user receives the Terms and Conditions.
2. Device Users must accept that they have read and agreed to the terms specified.
3. If Device Users do not accept the Terms, the registration process is aborted and the Device goes into the Terms Not Accepted state.
4. To resume activities, Device users need to close the enterprise store App.

8.2 Device Initiated Registration

This section describes the registration process through enterprise store. :

The generic process involves the following steps:

1. Enterprise store Download
2. Registration Request
3. Server Side Authentication and Verification
4. Terms and Conditions Acceptance

Device User initiates and completes the registration process. The entire process is driven on the device and the user need not leave the enterprise store.

Important: Some mobile browsers do not resolve the device OS, so it is recommended to use the device default browser only.

You can do device based registration for the following platforms:

- [iOS Device initiated Registration](#)
- [Android Device initiatedRegistration](#)
- [Windows Device 6.x Initiated Enrollment Registration](#)

8.2.1 Downloading Enterprise Store Using Kony Fabric Identity Console OAuth 2.0 Credentials

From Kony Management suite 4.2.5 onwards, if your enterprise is using Kony Fabric Identity service for OAuth 2.0, you can download the enterprise store using your enterprise credentials.

You can download an Enterprise store through two ways of authentication:

- Using Kony Management suite user login credentials
- Using Kony Fabric Identity Service OAuth 2.0 user login credentials

To download an enterprise store using Kony Fabric Identity Service OAuth 2.0 user login credentials, you must have Kony Fabric Identity Service configured in the Authentications Settings page of Kony Management Administrator console.

If the user in your Kony Fabric Identity Service OAuth 2.0 is not available in the Kony Management server, a new user is created.

When a new user is created, if the Kony Fabric Identity Service OAuth 2.0 is part of a group in OAuth 2.0, if the same group is present in Kony Management administrator console, the user will become part of the group in Kony Management administrator console.

In cases where multiple enterprise stores are configured and targeted to specific users or groups in Kony Management administrator console, during the process of downloading the enterprise store, the targeted enterprise store will download to the device.

Kony Fabric Identity service authentication is supported on iOS and Android devices. Kony Fabric Identity service authentication is not supported for Windows devices.

8.2.2 iOS Device initiated Registration

The entire process is driven on the device and the user need not leave the Enterprise Store. If registration is successful, the device should be registered and its status should change to Registered.

The generic process to register a device is as follows:

Note: In EMM 2.5 onwards, while registering iOS devices, all CSR requests from iOS devices are routed through EMM server to SCEP server.

Note: For iOS devices, enterprise store on a deactivated device from a previous enrollment, a user can enroll the device through enterprise store.

8.2.2.1 Authentication

1. To download the enterprise store from the Kony Enterprise App Store, the user must provide the following credentials:
 - a. Company Name (optional)
 - b. User name
 - c. Password

You can download an Enterprise store through two ways of authentication:

- Using Kony Management suite user login credentials
- Using Kony Fabric Identity Service OAuth 2.0 user login credentials

Important: Ensure that pop-ups are enabled in your web browsers. If pop-ups are not enabled, you may not see the log in page.

8.2.2.2 Server Side Authentication and Verification

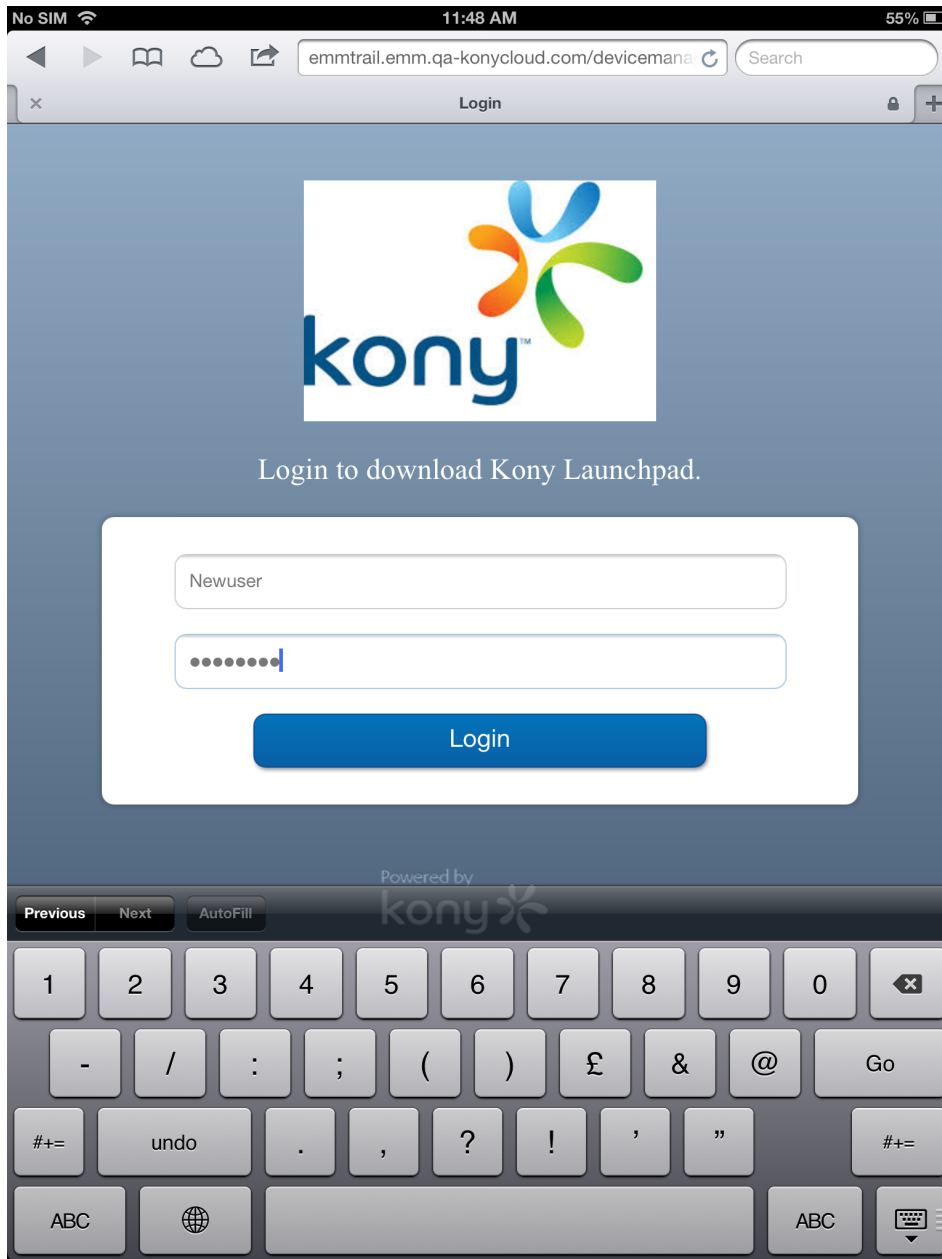
1. The details provided by the User are authenticated.
2. The EMM Server ensures that the device is not registered, not associated with any other user and allowed to enroll. Once this is ascertained, the server signals the agent to proceed with the enrollment.

8.2.2.3 Terms Acceptance

1. Once the authentication and verification is successful, the Terms and Conditions (T&C) are shown to the user.
2. The User must accept the terms specified. If the User does not accept the Terms, the registration process is aborted and the Device goes into the **Terms Not Accepted** state.

To perform iOS Device initiated Registration, follow these steps:

1. Enter application URL in the device based browser.



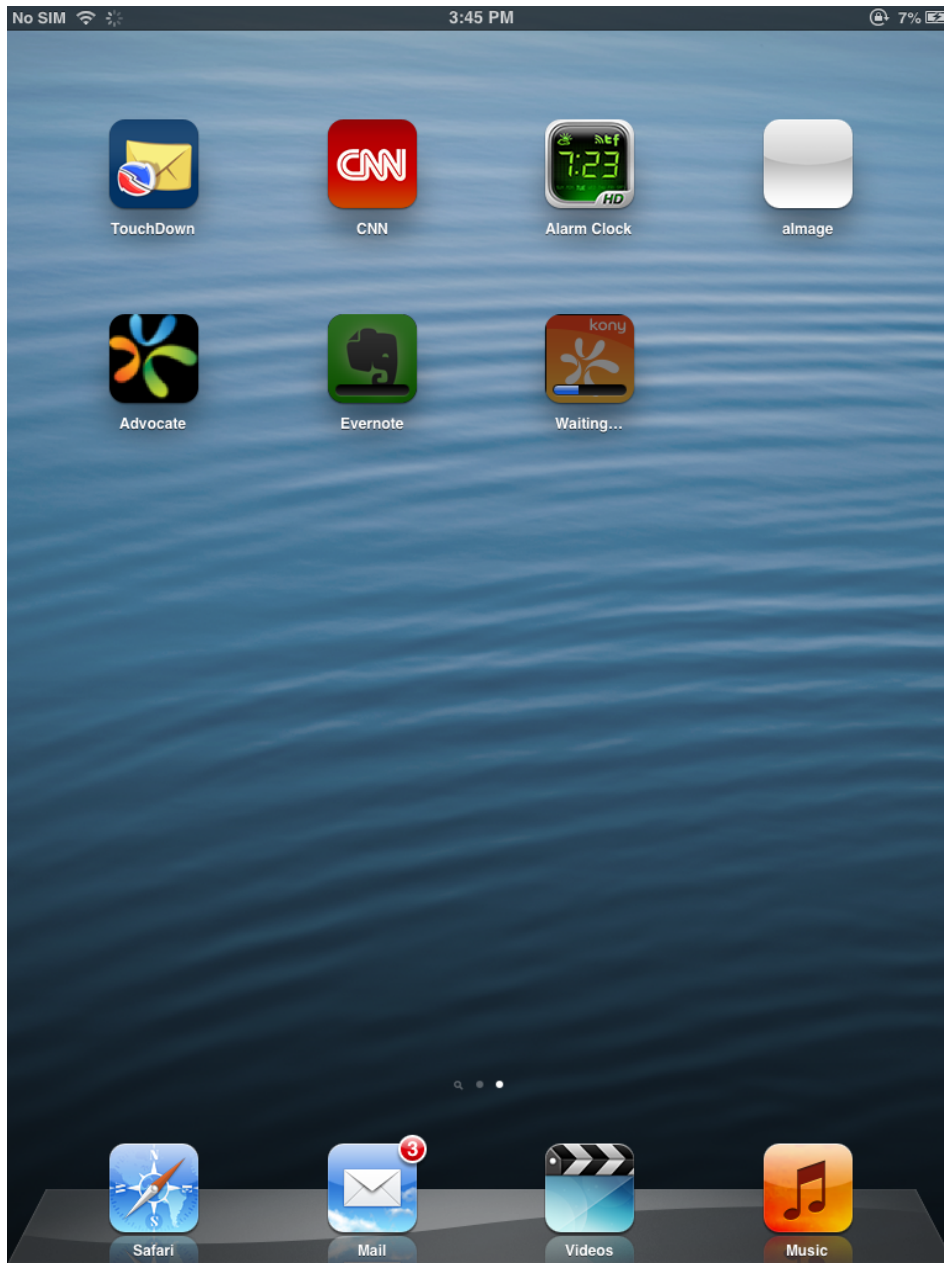
The Log-in page appears.

If JavaScript is turned off, the app logo image is not visible in the container download page in Safari browser.

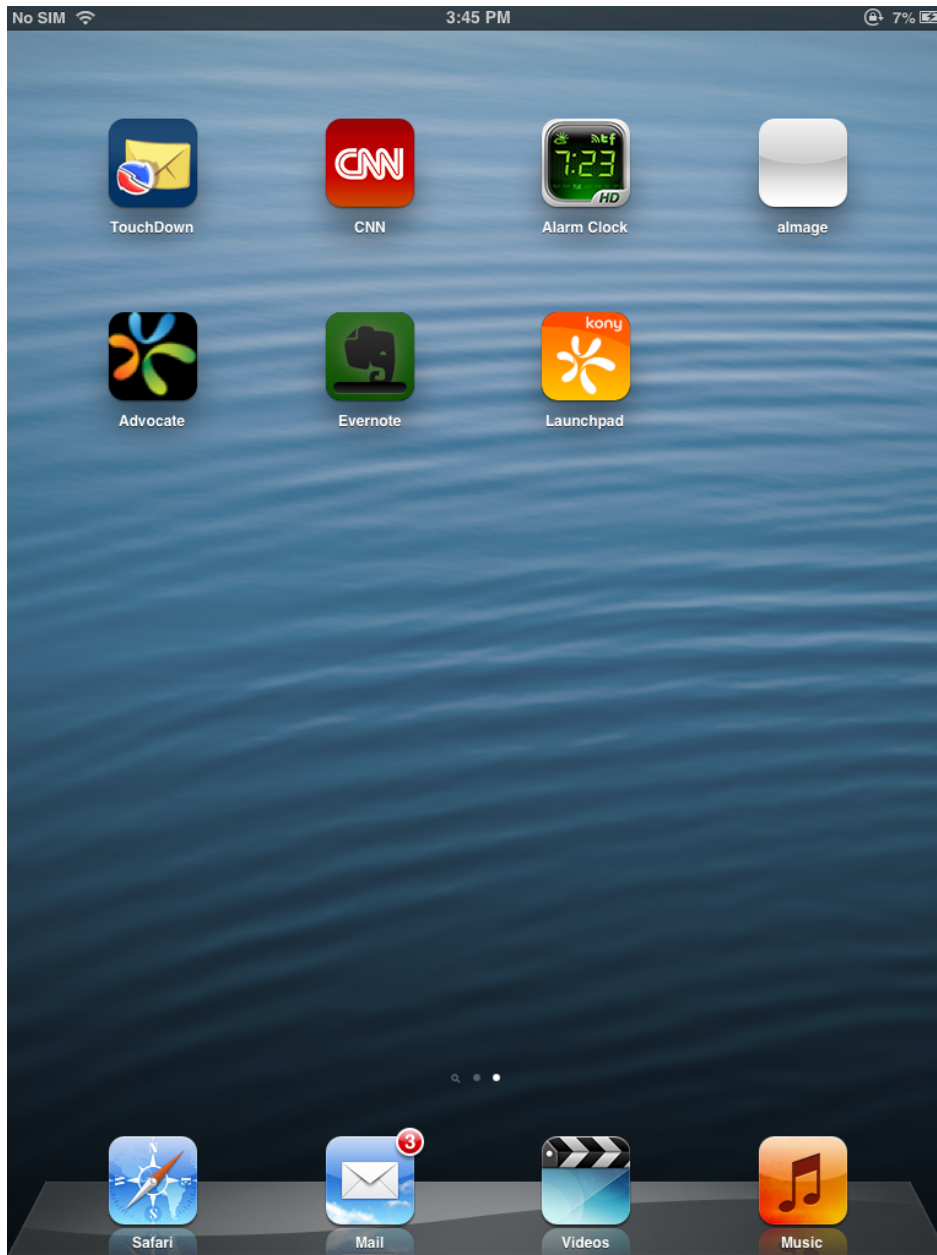
2. Enter your log-in credentials. These details are sent to the Server along with the device information.

Important: Based on users' existence in multiple ADs and sources, users need to provide domain and source details for authentication. For more details, refer to [Login > Authentication Scenarios](#)

3. After verifying the credentials the system displays the confirmation message. Click the **Install** button. The installation starts.

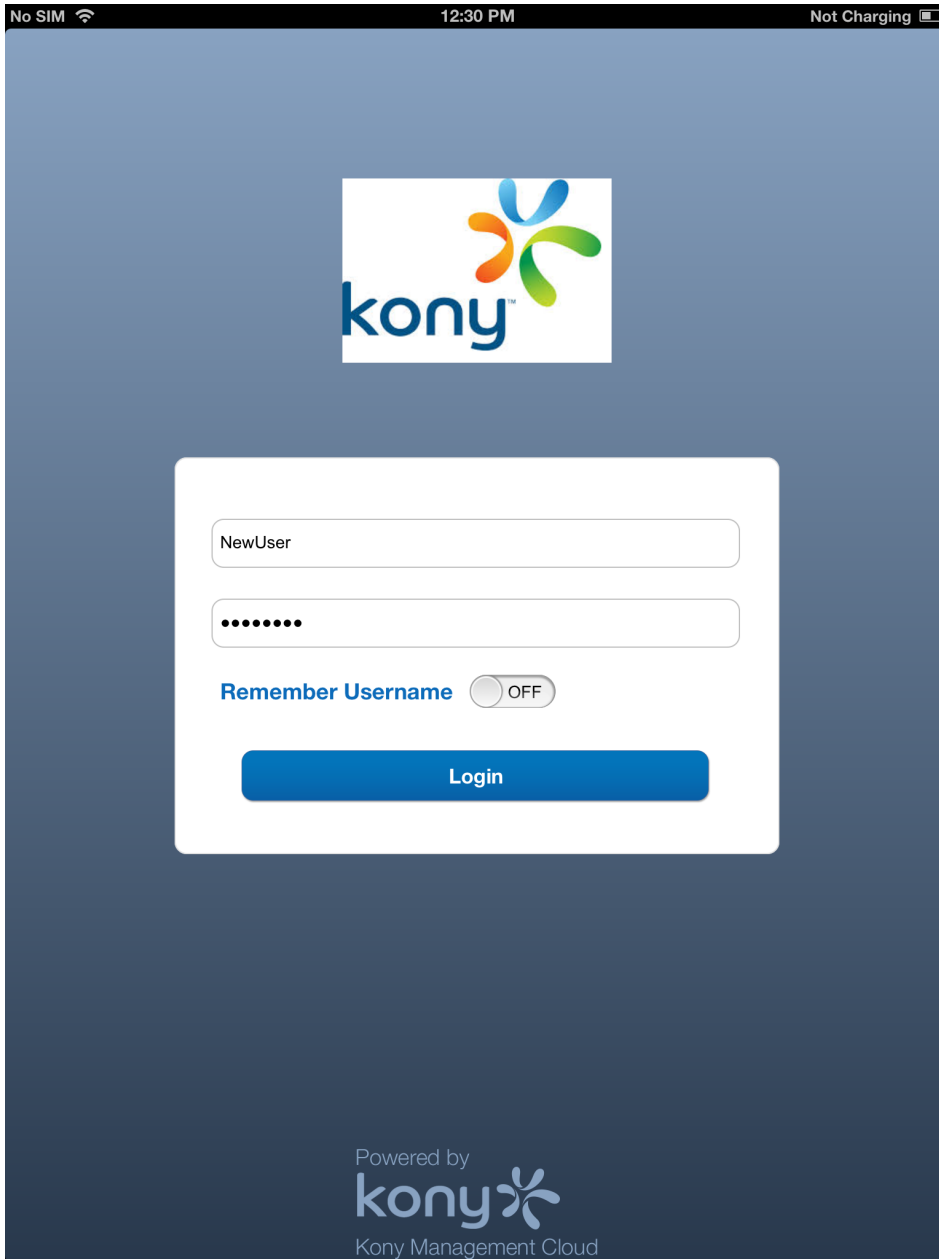


The above image indicates that installation process is in progress.



4. The enterprise store is installed on device.

Important: From iOS 9 onwards, a pop-up appears to trust the app profile. Navigate to **Settings > General > Profile > {Select Profile}** and then click on **Trust {Profile Name}**.



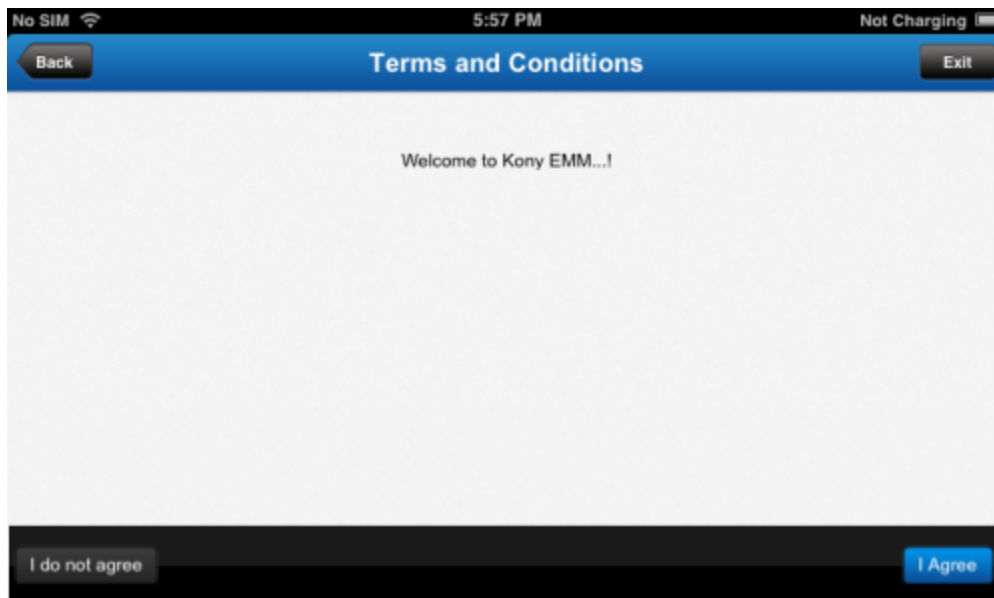
5.

Kony EMM Login page appears.

6. Enter your User Id and the Password.

Note: The Device Users is required to Authenticate themselves by providing User Name and Password. These details are sent to the Server along with the device information. The details provided by the User are authenticated. The EMM Server ensures that the device is not registered, not associated with any other user and allowed to register. Once this is ascertained, the server signals the agent to proceed with registration. If Verification fails, The Device goes into the status based on type of verification failure.

7. The system verifies the credentials. Once the authentication and verification is successful, system displays the Terms and Conditions.



8. You must accept that you have read and agree to the terms specified. Click the **I Agree** button. If you do not accept the terms, the registration process is aborted and the device goes into terms not accepted state. This marks the completion of the device registration.
9. The system displays the confirmation message. Click **OK** to proceed.

8.2.3 Android Device Initiated Registration

The entire enrollment is driven on the device, so a user need not leave the enterprise store. If registration is successful, the device is registered and its status changes to registered. The enterprise store has Administrator privileges over the device. The EMM server pushes policies and other requirements to the device.

Prerequisites: A device user uses an Android device and the device policy is defined. Your device user credentials must be present in the Active Directory.

To enroll a device, follow these steps:

8.2.3.1 Authentication

1. To download the enterprise store from Kony Enterprise App Store, a user must provide the following credentials:
 - a. Company name
 - b. Active Directory username
 - c. Password (Active Directory Password)

You need to enable cookies while downloading Kony EMM enterprise store.

You can download an Enterprise store through two ways of authentication:

- Using Kony Management suite user login credentials
- Using Kony Fabric Identity Service OAuth 2.0 user login credentials.

Important: Ensure that pop-ups are enabled in your web browsers. If pop-ups are not enabled, you may not see the log in page.

8.2.3.2 Server Side Authentication and Verification

1. The details provided by the user are authenticated.
2. EMM Server ensures that the device is not enrolled or associated with another user, and is allowed to enroll. Once these checks are complete, the server signals the EMM enterprise store to proceed with the registration.

8.2.3.3 Acceptance of Terms

1. Once the authentication and verification process is successful, the user views the terms and conditions.
2. The user must accept the terms specified. If the user does not accept the terms, the registration process is aborted, and the device goes into the **Terms Not Accepted** state.

To perform Android Device-Initiated Registration, follow these steps:

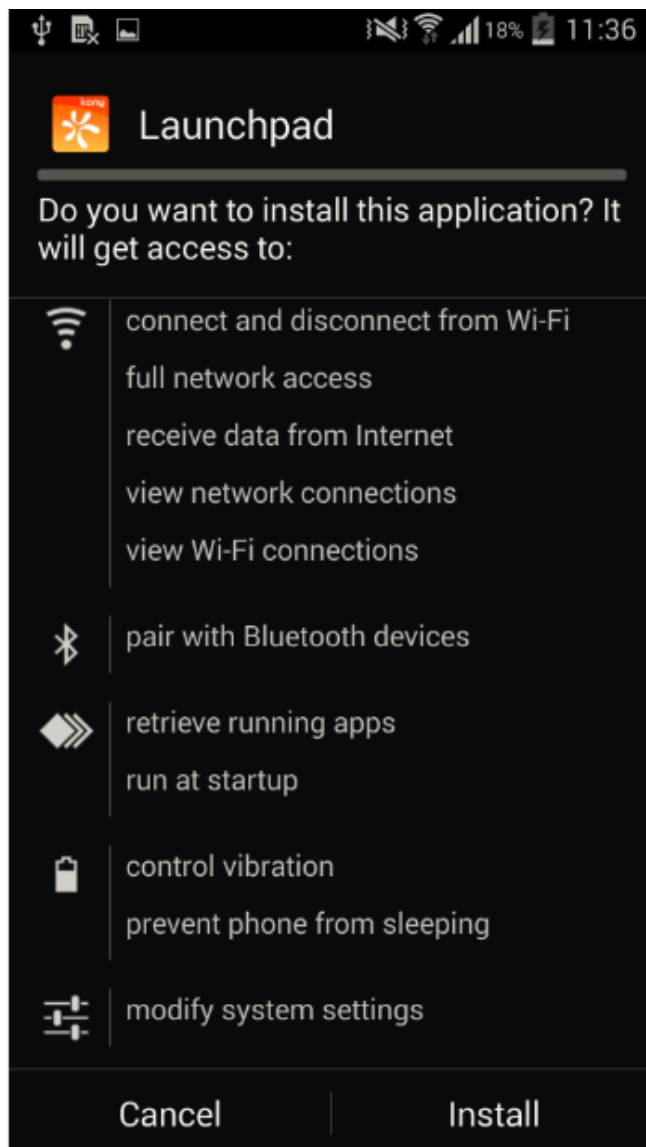
Prerequisite: A device user uses the device that should be registered. The device is an Android device.

1. Enter the application's URL in the device's browser.

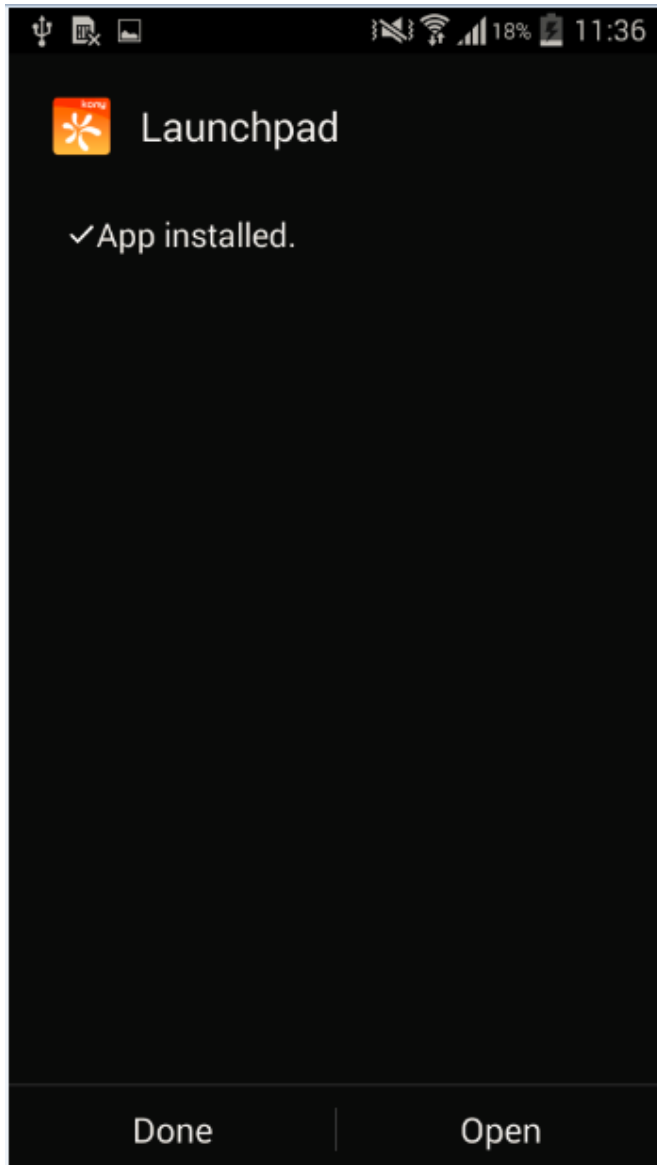
A log-in page appears.

2. Enter your log-in credentials. These details are sent to the server along with the device information

Important: Based on the existence of users in multiple active directories and sources, users need to provide domain and source details for authentication. For more details, refer to [Login > Authentication Scenarios](#).



3. Click the **Install** button. The installation starts.



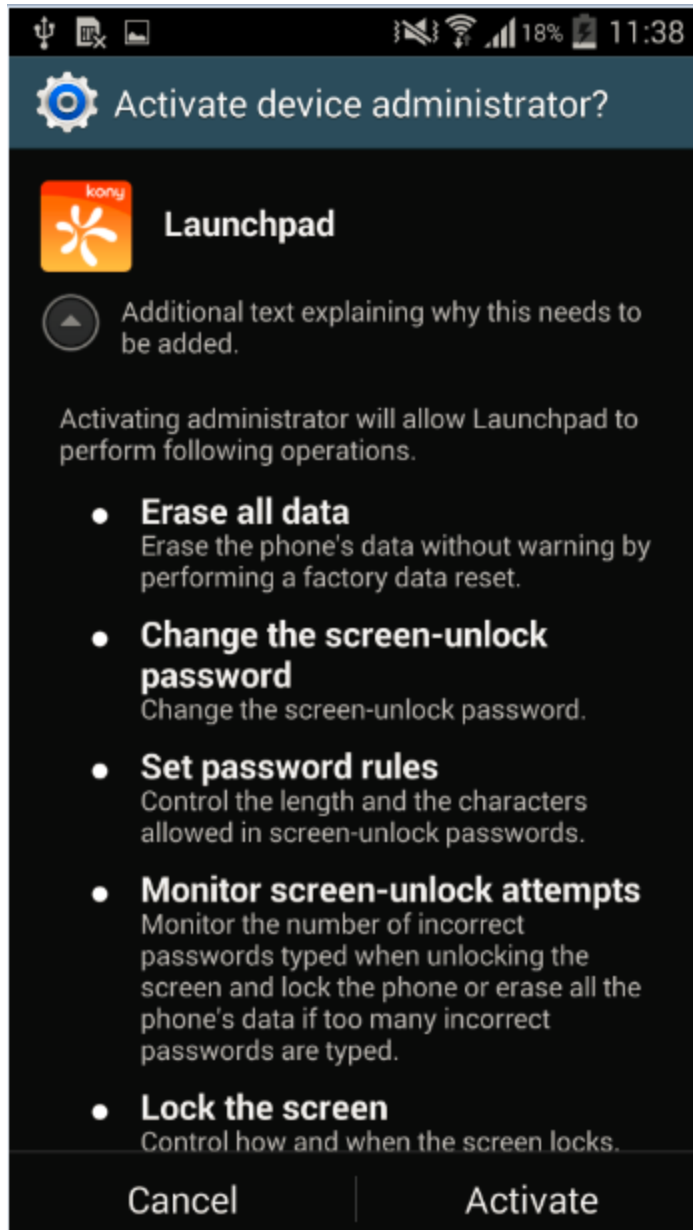
4. Click the **Open** button.
Kony EMM Login page appears.

5. Enter your credentials in Username and Password fields.

Note: The device users is required to authenticate themselves through usernames and passwords. These details are sent to the server along with the device information. The details provided by a user are authenticated. EMM Server ensures that the device is not and is allowed to register. Once the server completes this task, the server signals the agent to proceed with registration. If verification fails, the device's status reflects the type of verification failure.

6. The system verifies the credentials. Once the authentication and verification process is successful, the system displays the terms and conditions.
7. A user needs to read and accept the terms specified. Click the **I Agree** button.

If you do not accept the terms, the registration process is aborted. The device goes into the terms not accepted state.



8. A success message appears when the installation is complete. When a user wants to get support through the enterprise store, the communication is sent through email option only.

When you have a device that supports Android For Work, when you log into the enterprise store, you will receive a notification to create work profile. For more information on Setting Android For Work , see [Android For Work Email](#).

To create a work profile, do the following:

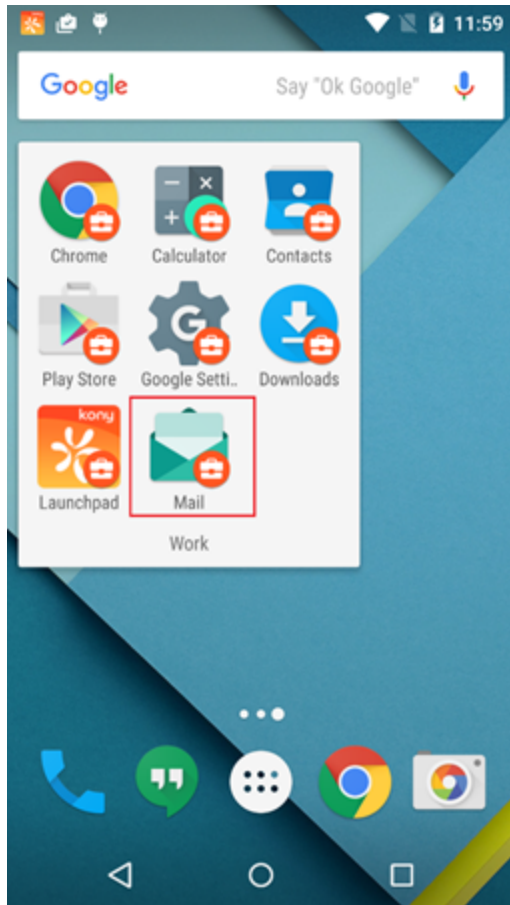
Once you create the work profile, if your Email policy for Android For Work Email is configured, you will receive a notification to download and install the Divide Productivity app.

Navigate to your Messages section and Actions in the enterprise store. Click on Download and Install Divide Productivity.

Google Play for Work store opens.

1. Touch Store Home.
2. Search for the Divide Productivity app.
3. Touch the app to select it, and then touch **Install**.
4. Review the requested access permissions and touch **Accept**.
5. After the app has installed, touch **Open**.
6. When asked if you want to configure Divide for your work domain, touch **Yes**
7. Enter your password for your work domain and touch **OK**
8. Once the Divide Productivity app is installed, you will get a notification to create Work email.

9. Follow the instructions on the screen. Work email is configured.



8.3 Enterprise Store

Kony Management Suite enterprise store is an app that is installed on a device to register it with EMM server. The Kony EMM enterprise store communicates with Kony EMM Server and carries out the instructions received from the server. Similarly, a user communicates with EMM administrators through Kony EMM enterprise store.

Important: Ensure that you upgrade to Enterprise Store of V8 GA release before upgrading your iOS device to iOS 11. If you upgrade to iOS 11 before upgrading the enterprise store, kill the enterprise store and download it again using your enterprise store download URL.

Important: For Android devices, the Enterprise store binary will be named based on the enterprise store name you provide. For example, if your enterprise store name is **Company App**, the .apk will be named as **CompanyApp.apk** for Android phones and **CompanyApptablet.apk** for Android tablets.

Ensure that the Enterprise store name you provide (in the Branding section) does not contain # sign in it. If the Enterprise store name has a # sign in it, downloading the enterprise store on the Samsung native browser will fail.

Kony EMM enterprise store steps up security with several new checks for app tampering and app integrity.

For Windows Phone 8.X, if the enterprise store is deleted, it will be installed automatically in the next heartbeat. Deleting enterprise store does not affect enrollment status.

When the EMM server is down, the enterprise store will behave as it is offline.

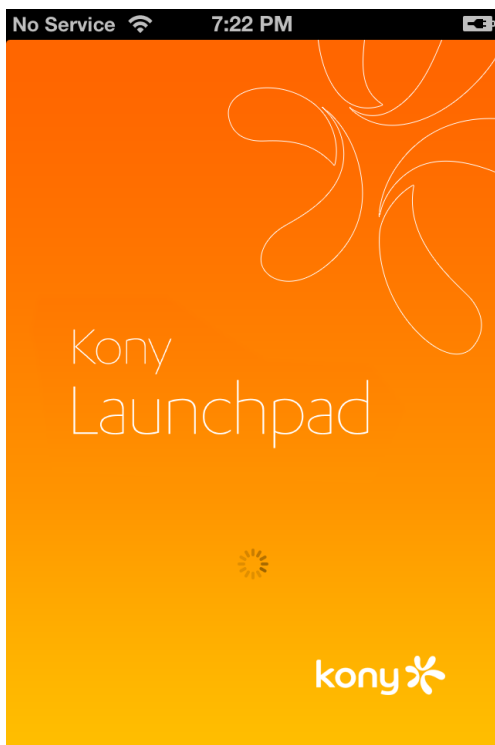
- Resources that require an online connection will no longer be available.
- An app that is not installed on the device will not be available in the apps tab.
- Content that is not downloaded to the device will not appear in the content tab.

- Messages will not be available.
- A banner that enterprise store is offline will appear within the enterprise store.

8.3.1 Splash Screen

When the enterprise store App is launched, a splash screen is shown to the user.

8.3.1.1 iOS



8.3.1.2 Android



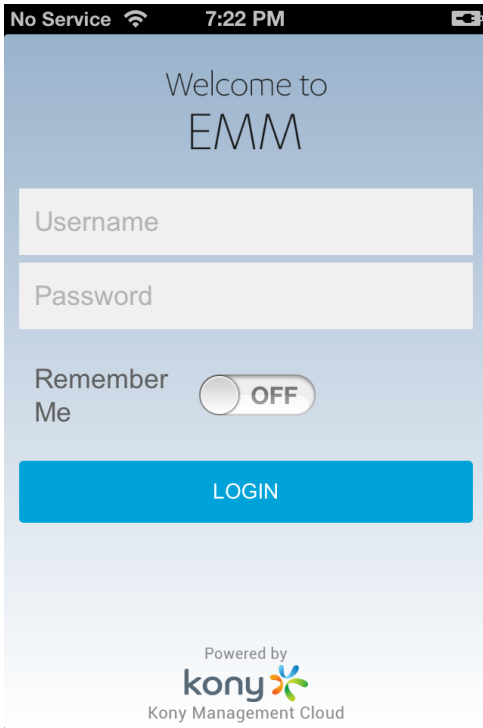
8.3.1.3 Windows Phone 8.X



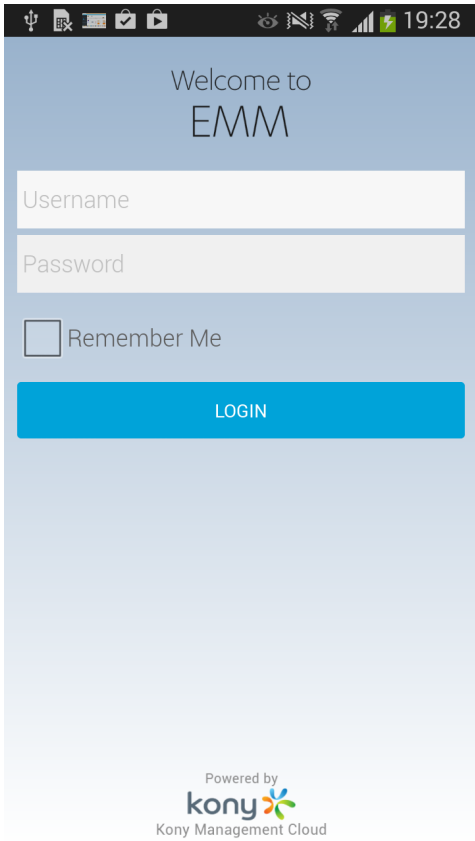
8.3.2 Log-in Screen

Once enterprise store is launched, the user lands on the log-in page and must provide log-in credentials to use the app. The log-in pages for iOS and Android devices are shown below.

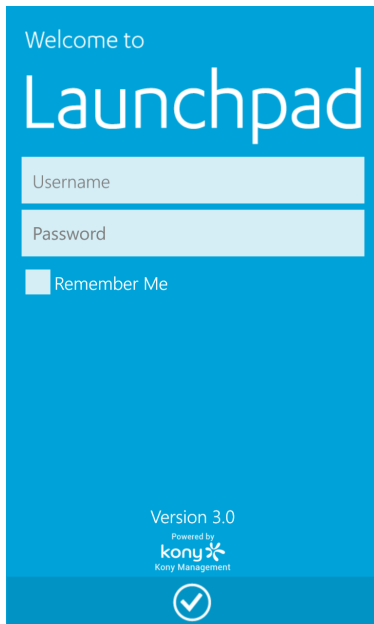
8.3.2.1 iOS



8.3.2.2 Android



8.3.2.3 Windows Phone 8.X

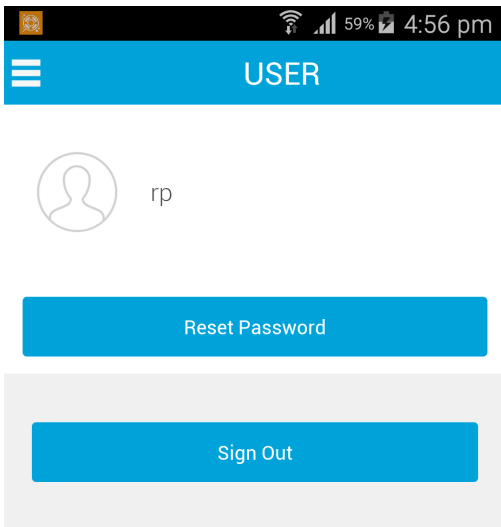


Kony EMM enterprise store has six tabs:

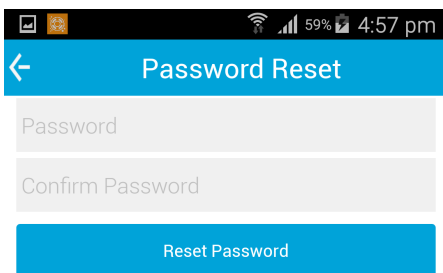
- [User](#)
- [Store](#)
- [Content](#)
- [Messages](#)
- [Support](#)

8.3.3 User

Displays the User details. You can sign out from the enterprise store from here.



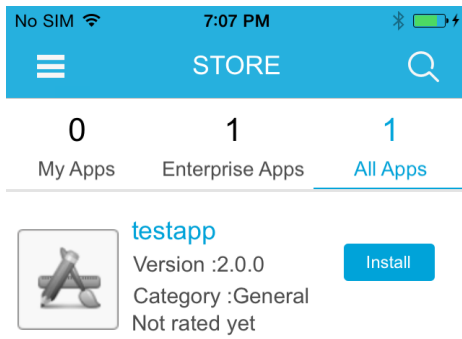
When you click the reset password button, reset page appears.



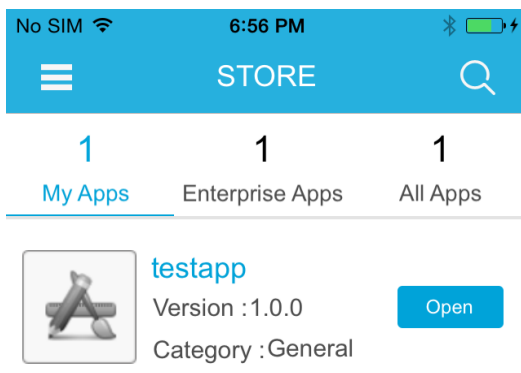
8.3.4 Store

Once an app is published, the administrator pushes that app to the App Store. You can browse enterprise apps from the store, and select the required applications to download and install on your device. Applications that are targeted to a specific group or user are displayed only to them in the store.

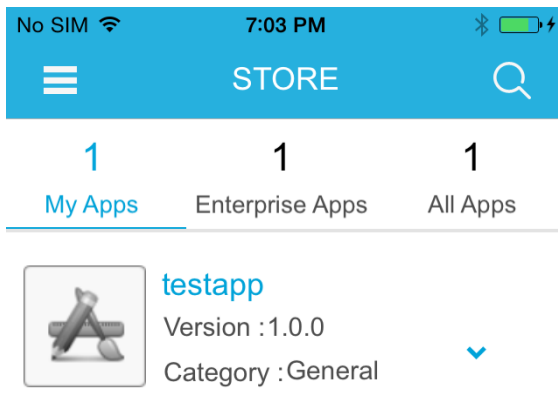
Store is not available if the device is offline.



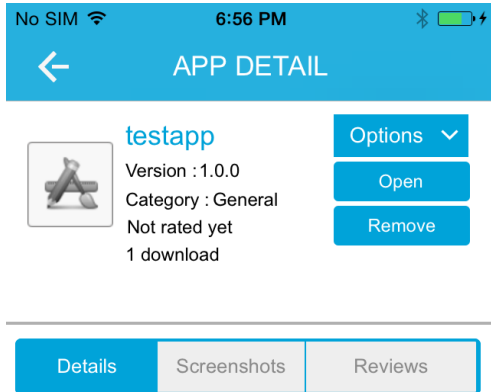
In All Apps, all targeted apps are available, including wrap and sign, and sign-only apps. A user can choose to install the targeted app.



Once an app is installed, it appears in the My Apps page. The administrator can open the My Apps page to use the app.



If there is an upgrade for the selected app, the more options **V** button appears. Click the more options button to see the **Open** and **Update** options.

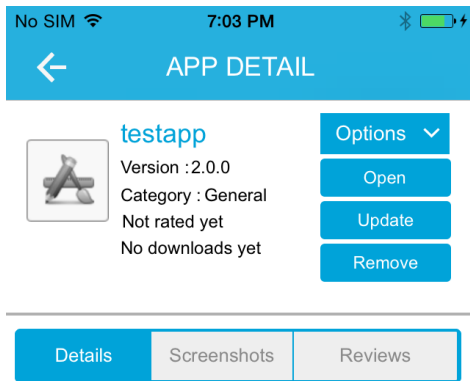


No Description Available

In the **App Details** page, two options are shown - **Open** and **Remove**.

The **Description** pane contains three tabs - **Details**, **Screenshots**, and **Reviews**.

- The **Details** tab contains any description provided for an app, and links to guidebooks.
- The **Screenshots** tab contains screen shots of an app.
- The **Reviews** tab contains reviews posted for an app Users can rate and review apps in this tab.



No Description Available

If there are updates to an app, the **Update** button appears under Options.

8.3.4.1 My Apps

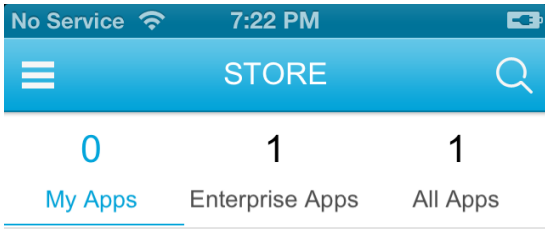
This tab displays all applications that are installed and can be installed on your iOS or Android device. An **Install** button displays for each application. If the application is already installed, then the **Launch** button appears.

You can launch installed apps on your device only through the My Apps screen. If an app is not required, you can uninstall it from your device.

This tab is available even if the device is offline.

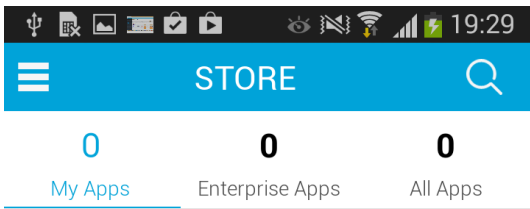
Important: If a device experiences software upgrade issues and location services flip between On and Off, apps may launch. This condition has been seen in the Samsung Galaxy 54.

8.3.4.2 iOS



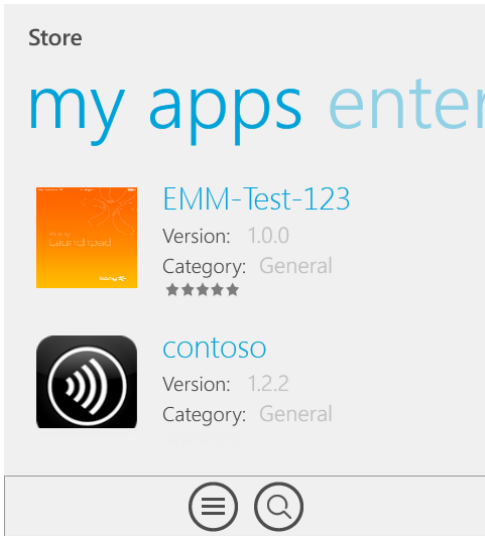
No Apps Available

8.3.4.3 Android

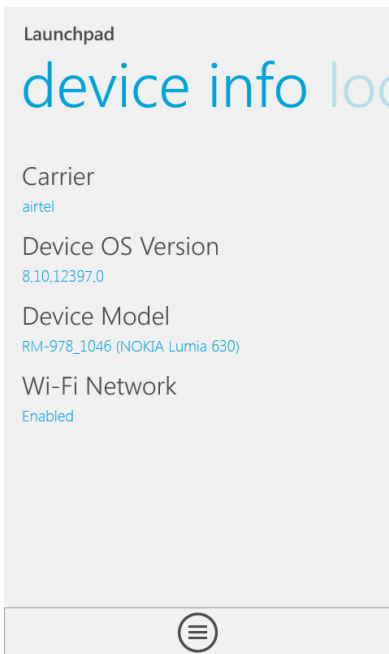


No Apps Available

8.3.4.4 Windows Phone 8X



Windows Phone 8X

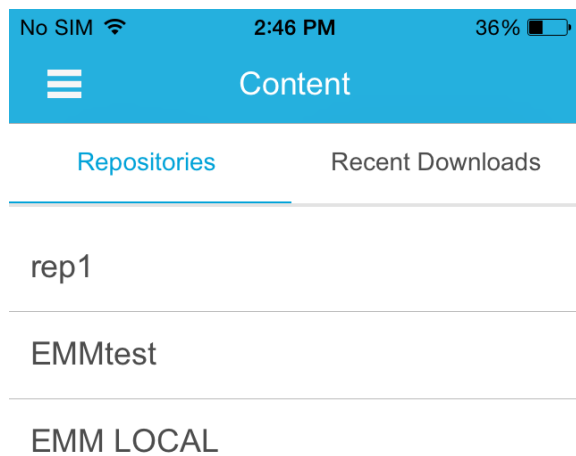


8.3.5 Content

Content management is available for iOS, Android, and Windows 8.1 devices. On devices, users can view the content targeted by the EMM administrator, content the users uploaded to their user space through the self-service console, and content shared with the current user by other users.

Users can view but not modify the content. On Android phones, if a user modifies the content, the changes are not synced back to the server. The version on the server will be pushed to the device automatically and overwrite any changes made locally on the device.

Content Tab displays two tabs, Repositories and Recent Downloads.

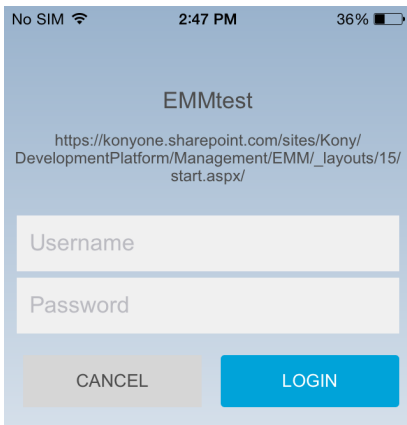


The repositories tab displays the available repositories for the user. These include the local emm directory as well as any SharePoint repositories targeted to the user by an enterprise administrator.

- [SharePoint Repository](#)
- [Local Repository](#)

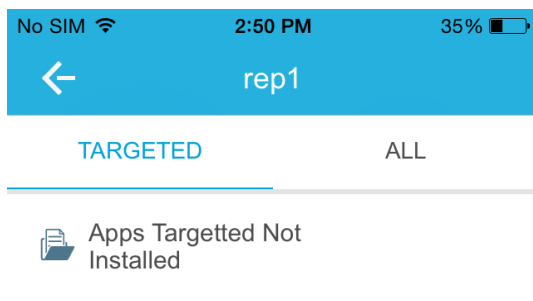
8.3.6 SharePoint Repository

When you click a SharePoint repository the SharePoint login screen appears. To access your SharePoint, enter your SharePoint login credentials. Once you enter your credentials, the Content tab appears.

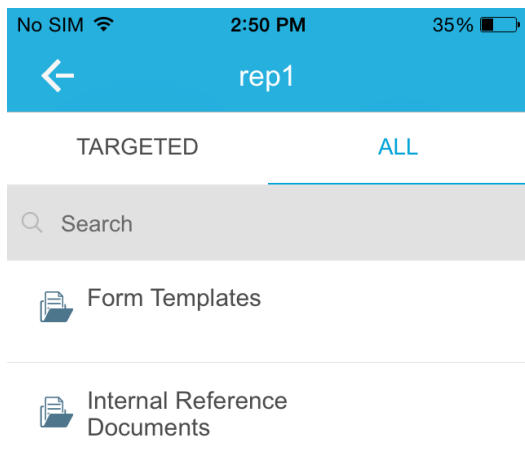


The Content tab for SharePoint repositories displays two tabs.

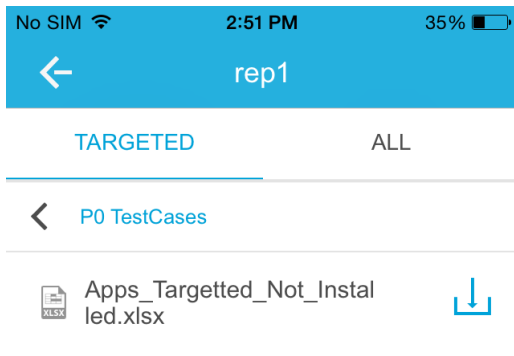
- **Targeted** : Displays content that is targeted to the user or the group.



- **All**: Displays content that the user has access to in SharePoint. You can search for any files in your SharePoint repository from the **All** tab by using the **Search** field.



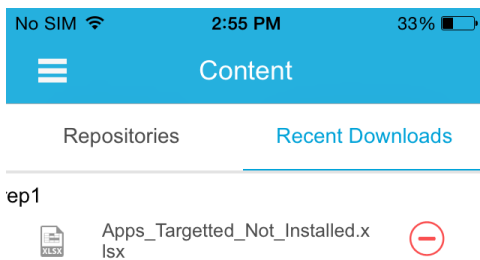
You can download any file that is available to you by tapping on the download button.



When you download a file, an alert appears notifying you that you can now access the file offline on the device.

8.3.7 Recent Downloads

The Recent Downloads tab displays the files that you have downloaded recently. You can delete any of these files from the device directly from this tab.



8.3.8 Local Repository

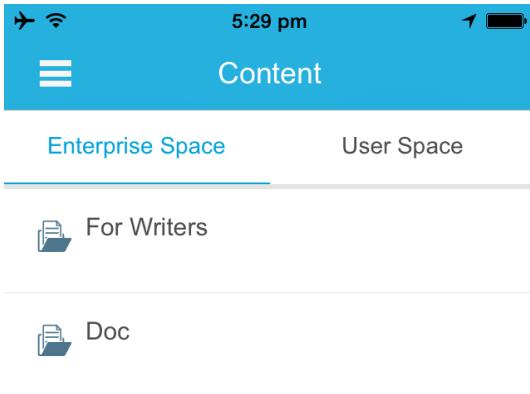
The content tab for a local repository displays two tabs:

Enterprise Space: Displays the content shared with a user by the enterprise and other users. Content is available only for iOS and Android devices.

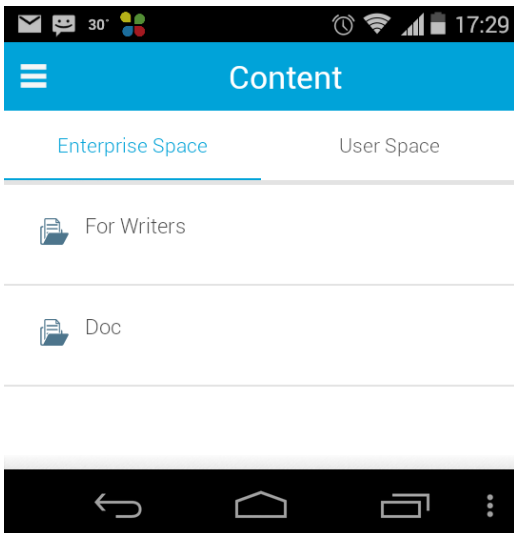
User Space: Displays content uploaded by a user to a self-service console.

In case of iOS, various policies can be applied to the content targeted by the administrator. For Android and Windows 8.1 devices, the administrator can use just one policy, **Allow Access in Android** or **Allow Access in Windows**.

8.3.8.1 iOS



8.3.8.2 Android

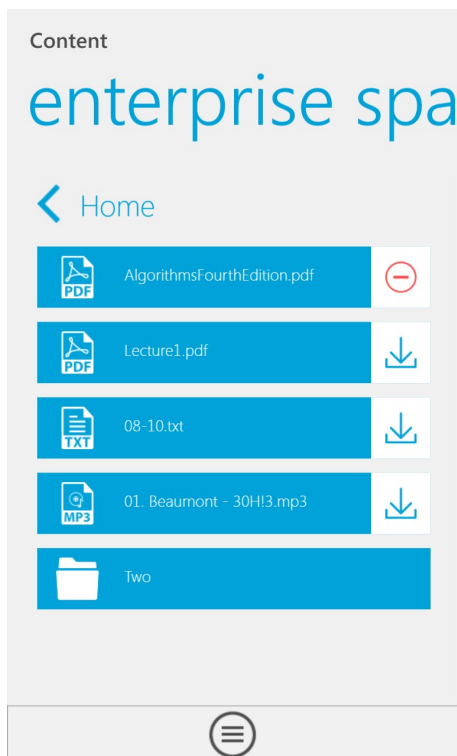


When a user downloads a document, on Android devices, the document is downloaded to the device. For iOS devices, the file is downloaded within the enterprise store and is available for a user even when the device is offline.

8.3.8.3 Windows Phone 8.1

On Windows Phone 8.1 devices, you cannot pause a document download.

- If you initiate a download and then kill the enterprise store, the download will continue to run in the background. During the content download process, if your device loses network, download will wait and resumes when the network is restored.
- You can download two files at the same time on Windows Phone 8.1. Any request for more downloads will be in queue and will initiate once one of the downloads completes.

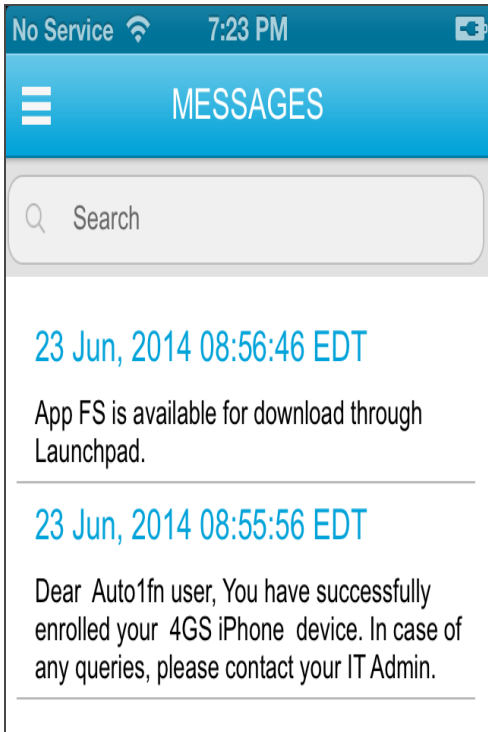


8.3.9 Messages

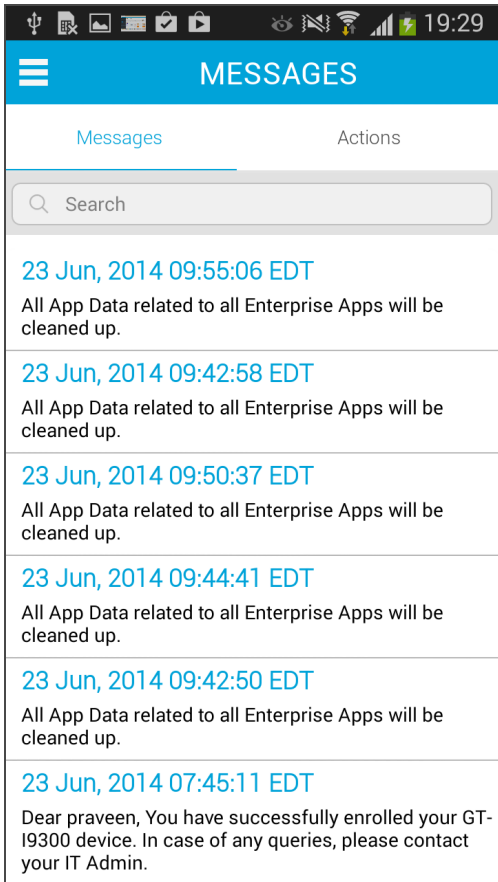
This tab contains all the push messages sent to the respective device. It may pertain to any issue, such as newly available apps and so on.

This tab is not available if the device is offline.

8.3.9.1 iOS



8.3.9.2 Android



On enterprise store for Android, the Messages section has two tabs:

- **Notifications** - All regular push messages are shown in Notifications tab.

8.3.10 Deleting an Enterprise Store

In iOS, a user can delete enterprise store, but the device will not be [Control Removed](#). As the device is still registered, all policies, apps, and settings remain on the device. Deleting enterprise store does not affect enrollment status.

To get enterprise store again, the user can go enterprise store download URL, authenticate with login details, and then download enterprise store.

In case of Android, in order to delete enterprise store, admin privileges must be removed for enterprise store. Thereby sending into to [Control Removed](#) status. Therefore all policies and apps and settings are removed. If a user wants to be part of EMM, the user must re-register into EMM.

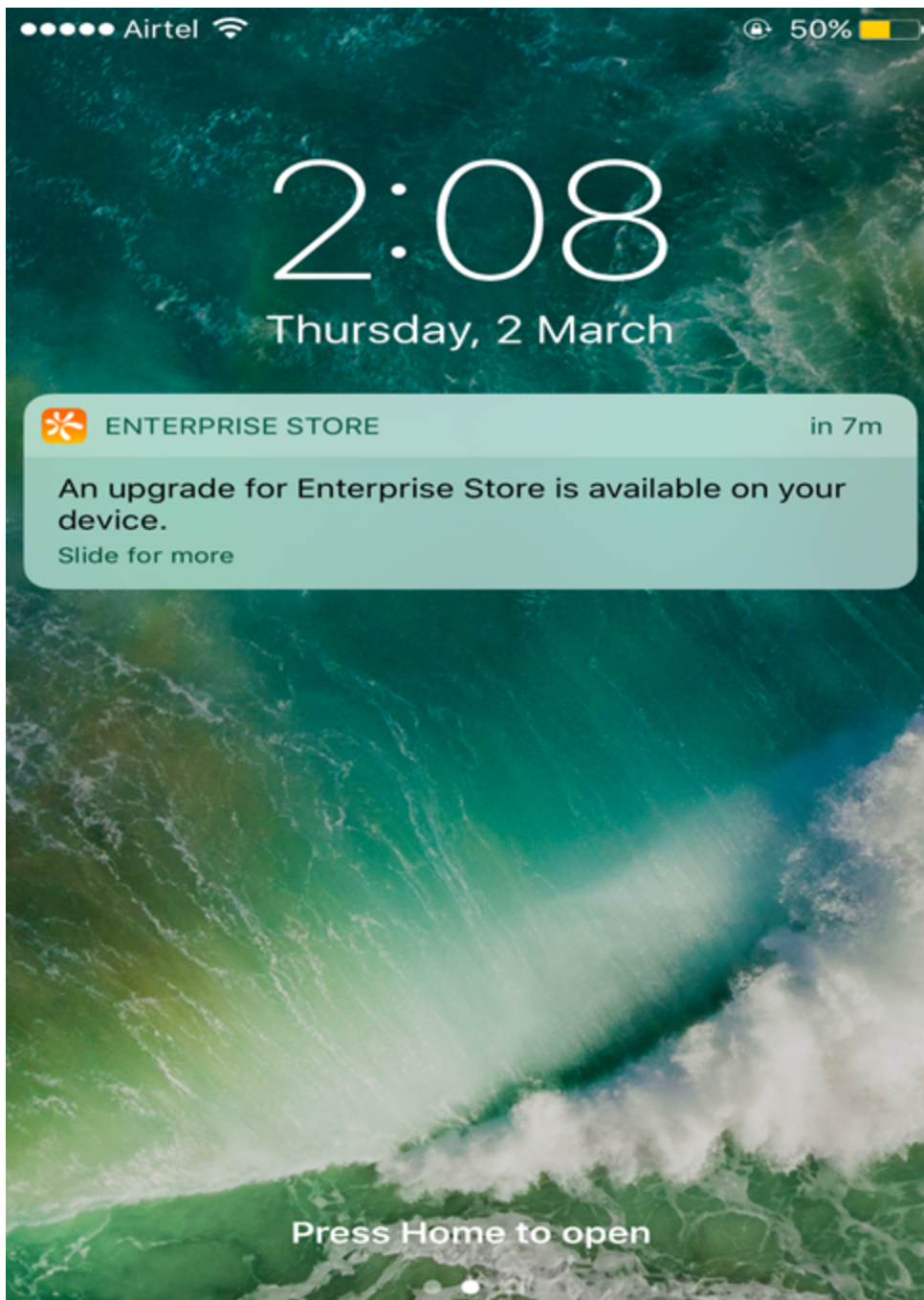
Note: In case of Windows 8X devices, if enterprise store is deleted, but the device is still enrolled in EMM, enterprise store will be installed silently on next heartbeat.

8.3.11 Enterprise Store Upgrade

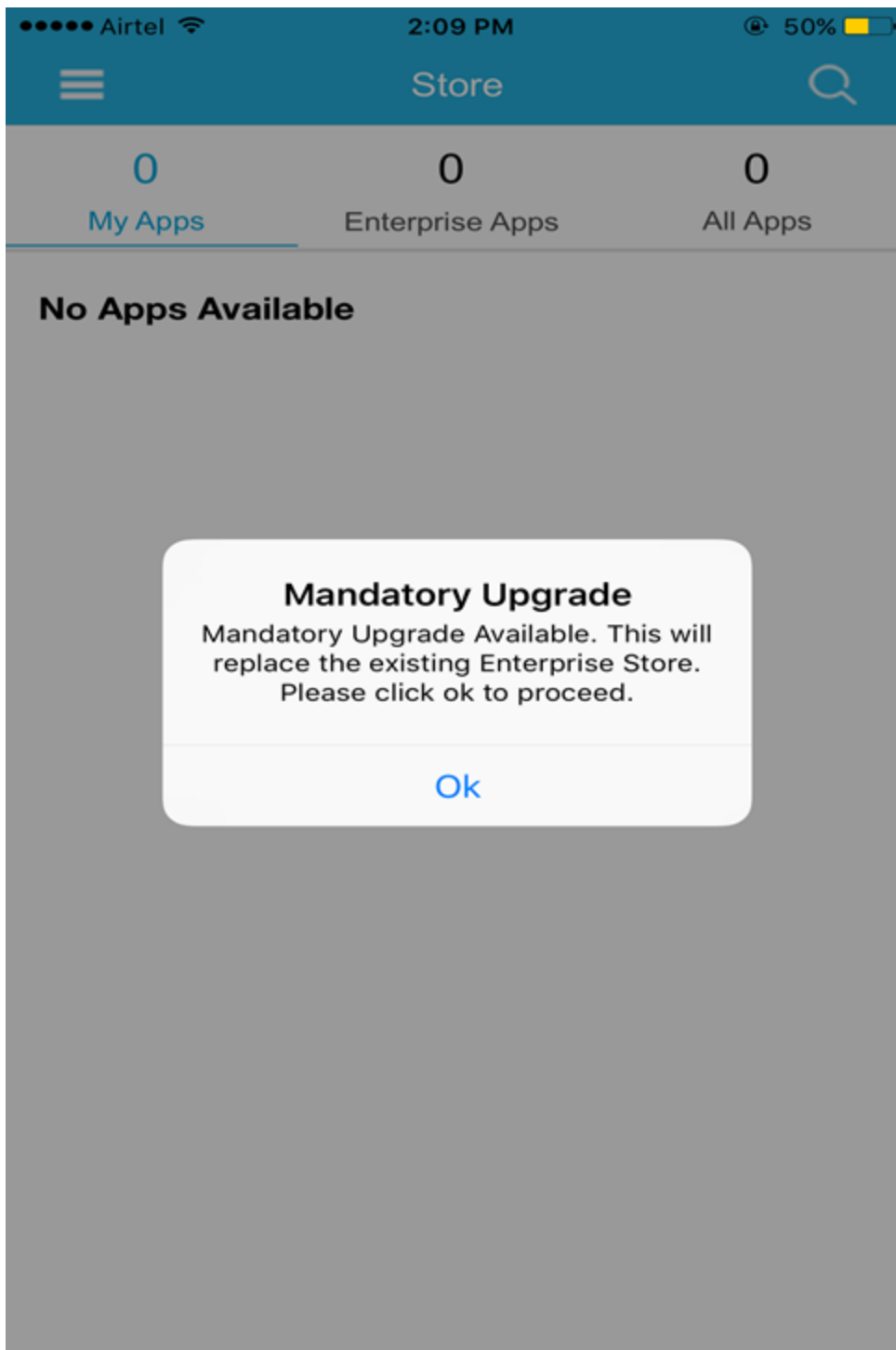
Whenever an enterprise store is upgraded, devices will receive a notification about the upgrade. It is mandatory to update the enterprise store to the latest version.

8.3.11.1 Upgrade Enterprise Store in iOS

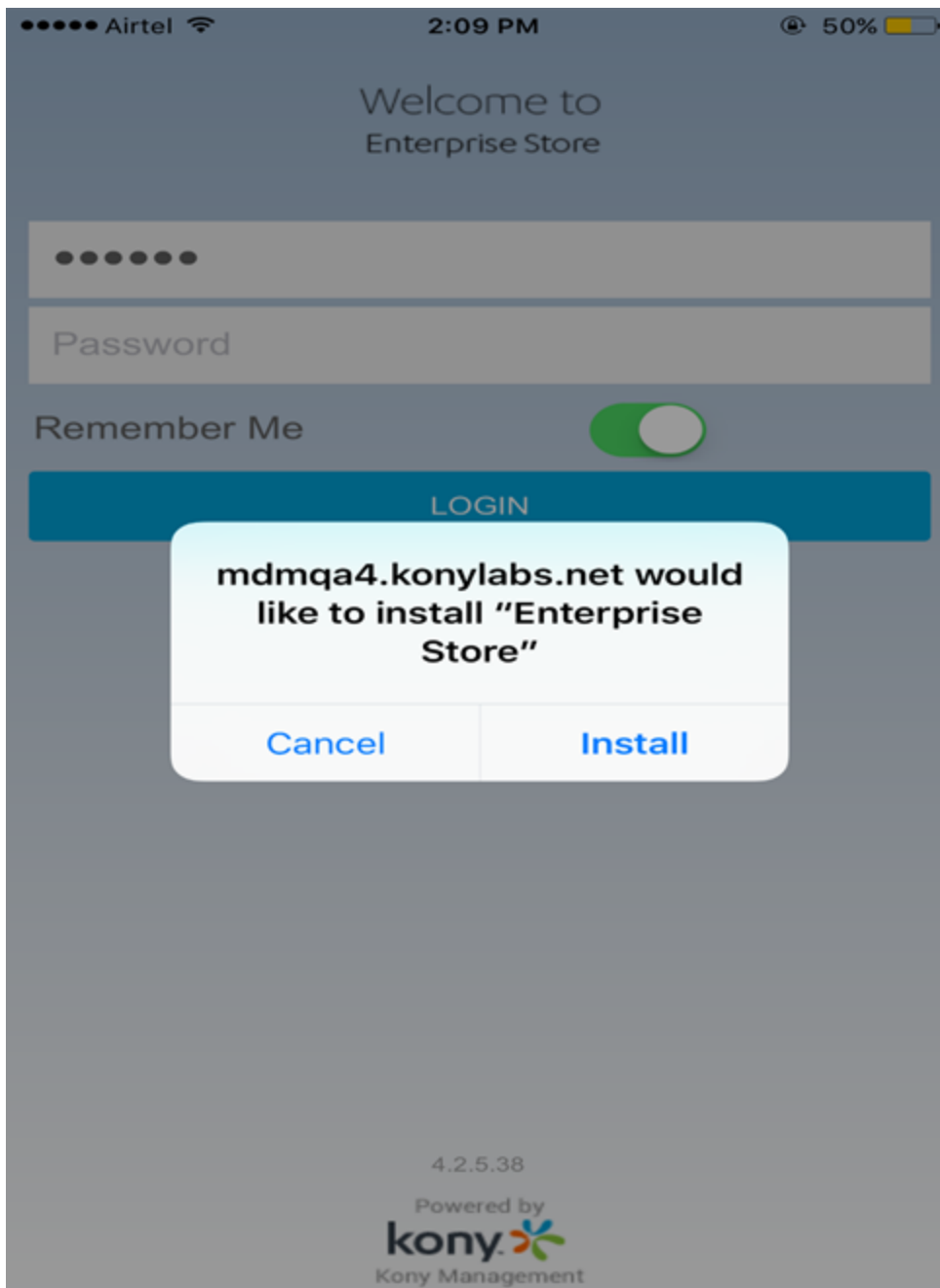
When you have an update available for your enterprise store in iOS, you will receive a push message.



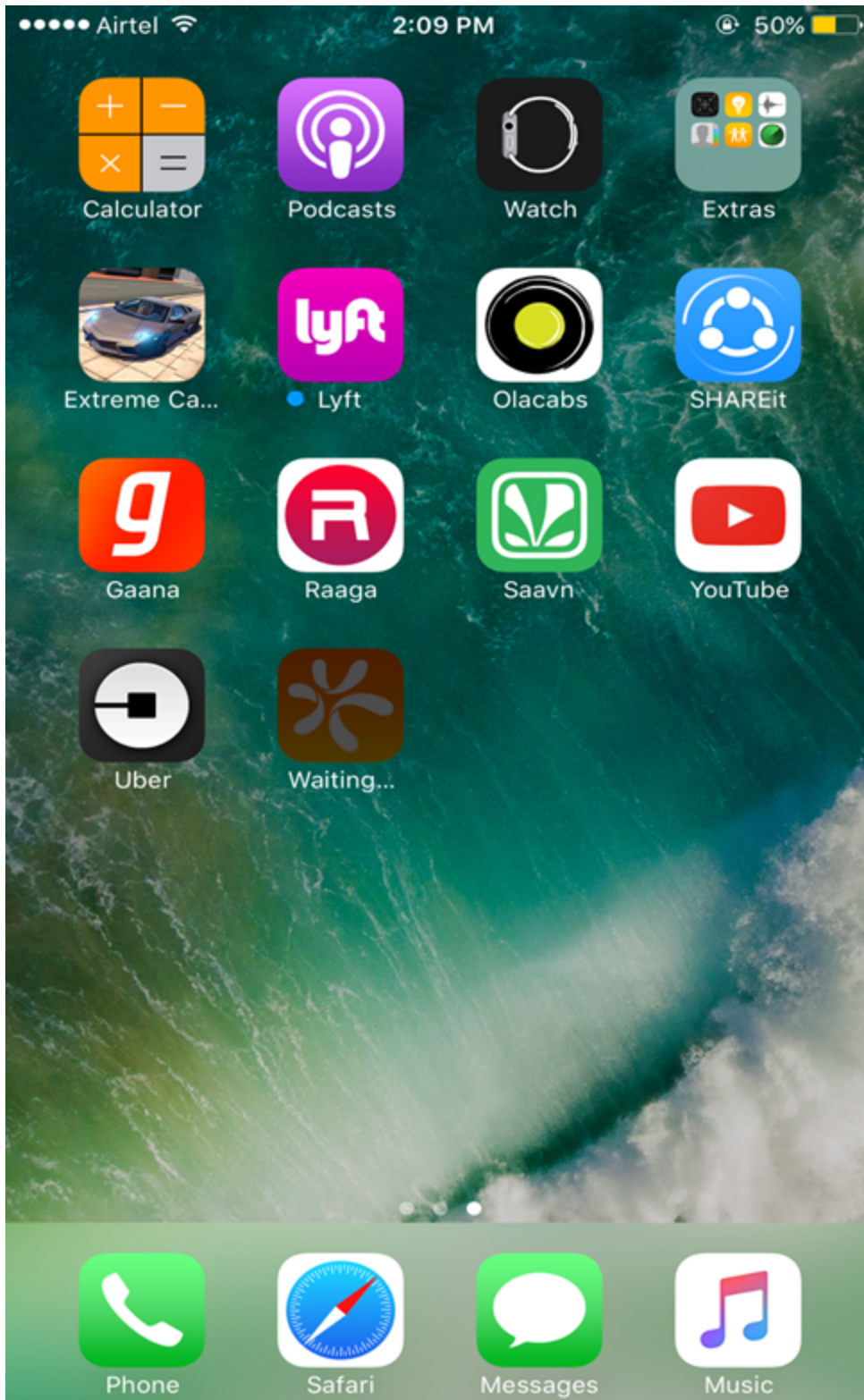
Once you log in to the device, a mandatory upgrade message appears.



Once you click **Ok**, an Install message appears.

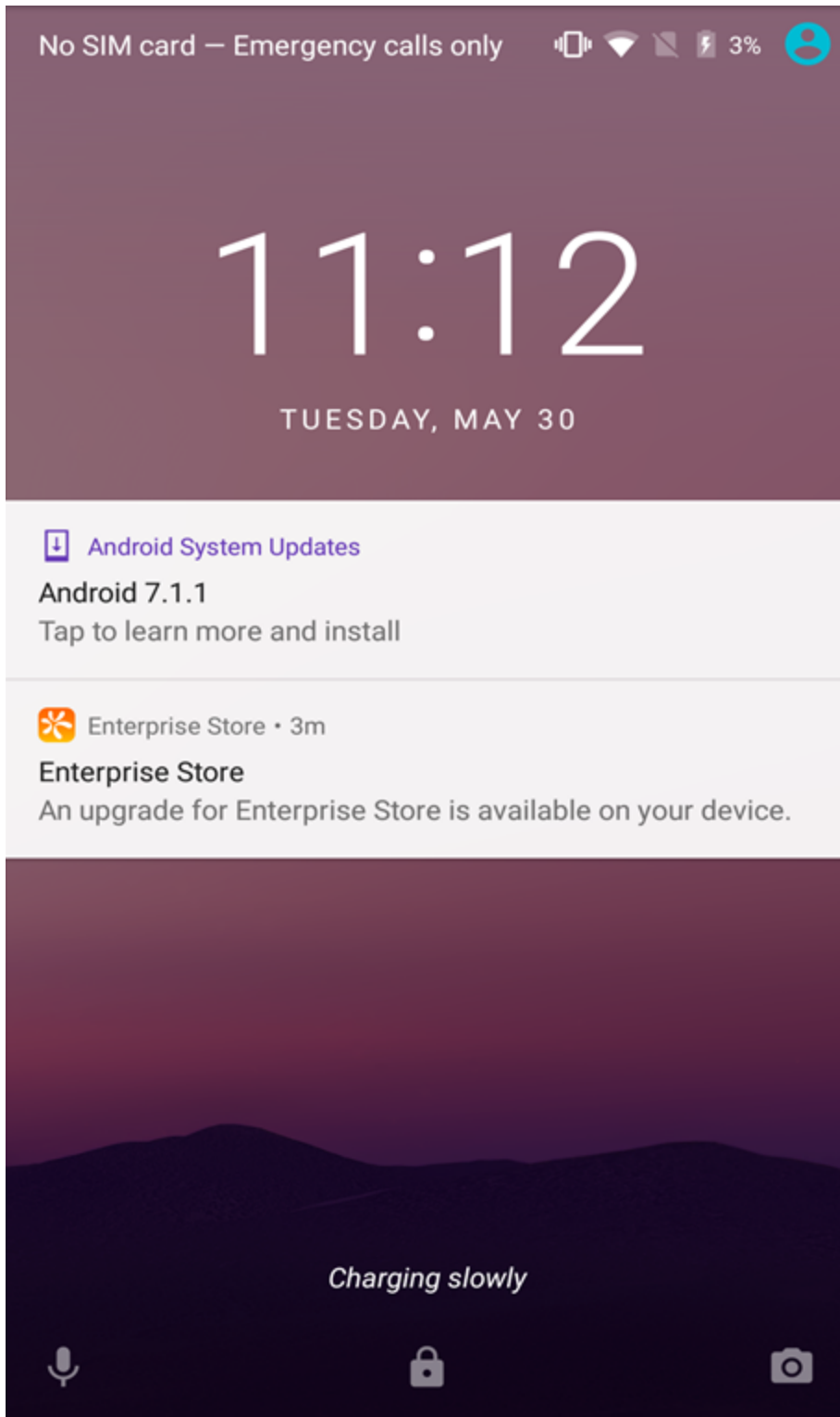


Click **Install**. Screen goes back to the home page and the enterprise store is installed.

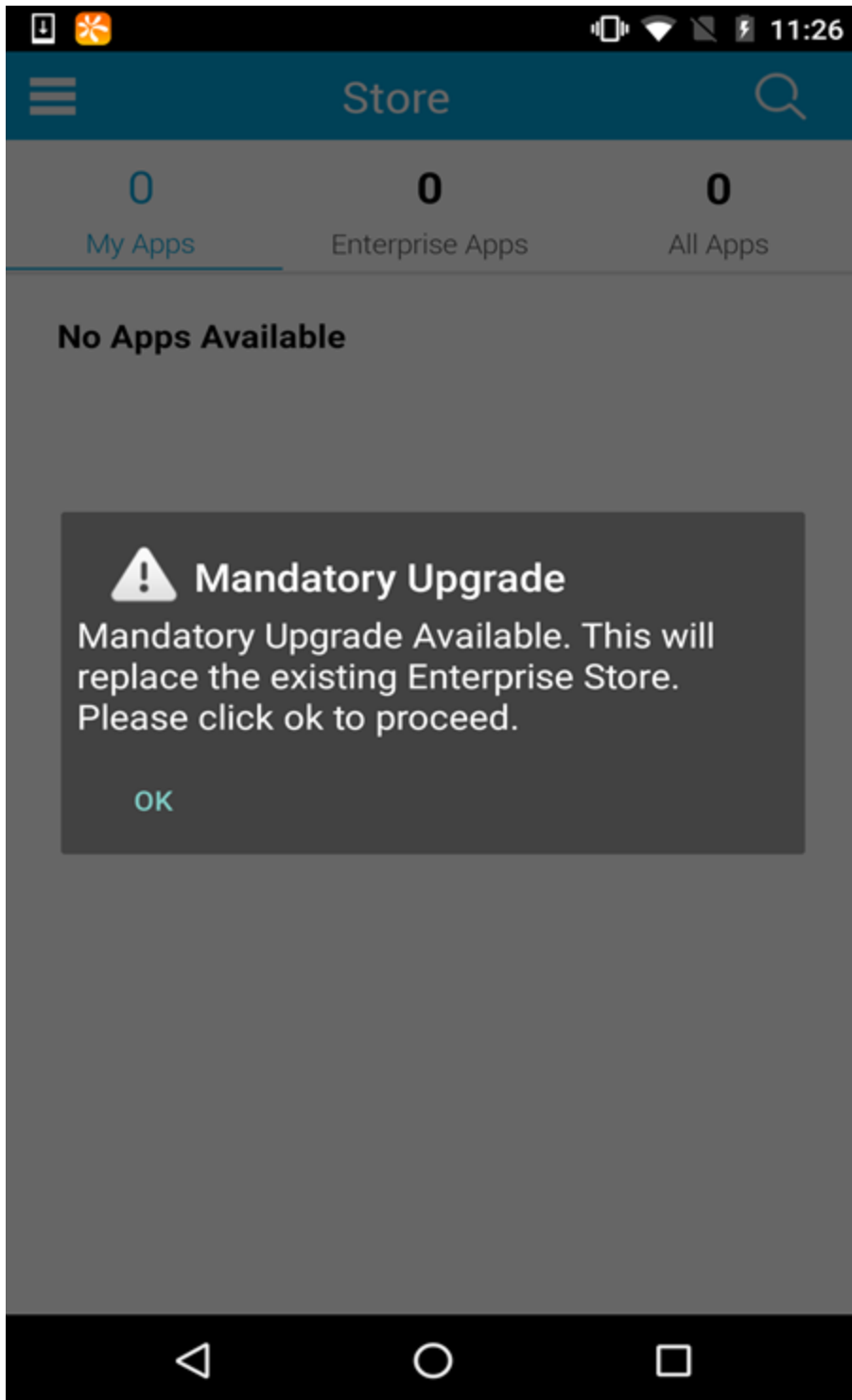


8.3.11.2 Upgrade Enterprise Store in Android

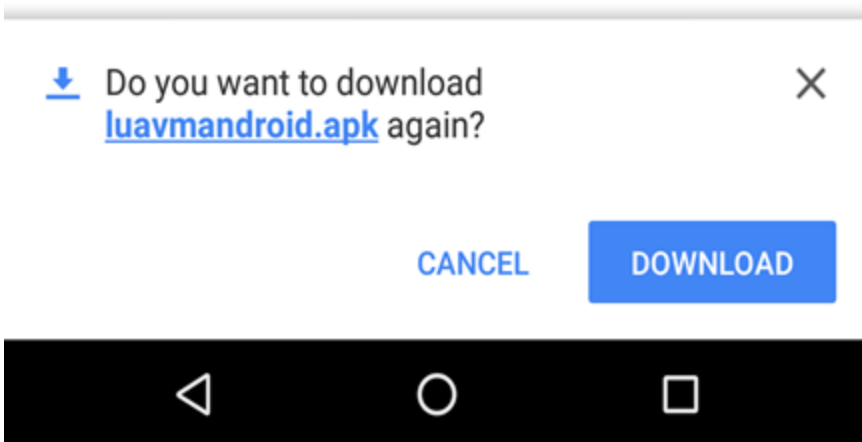
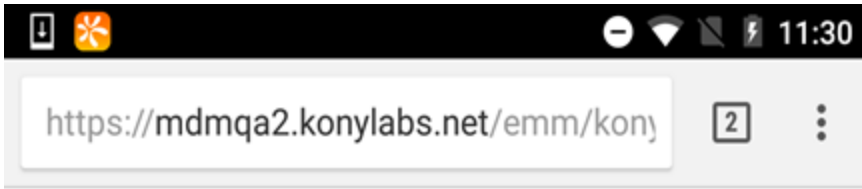
When you have an update available for your enterprise store on your Android device, you will receive a push message.



Once you log in to the device, a mandatory upgrade message appears.

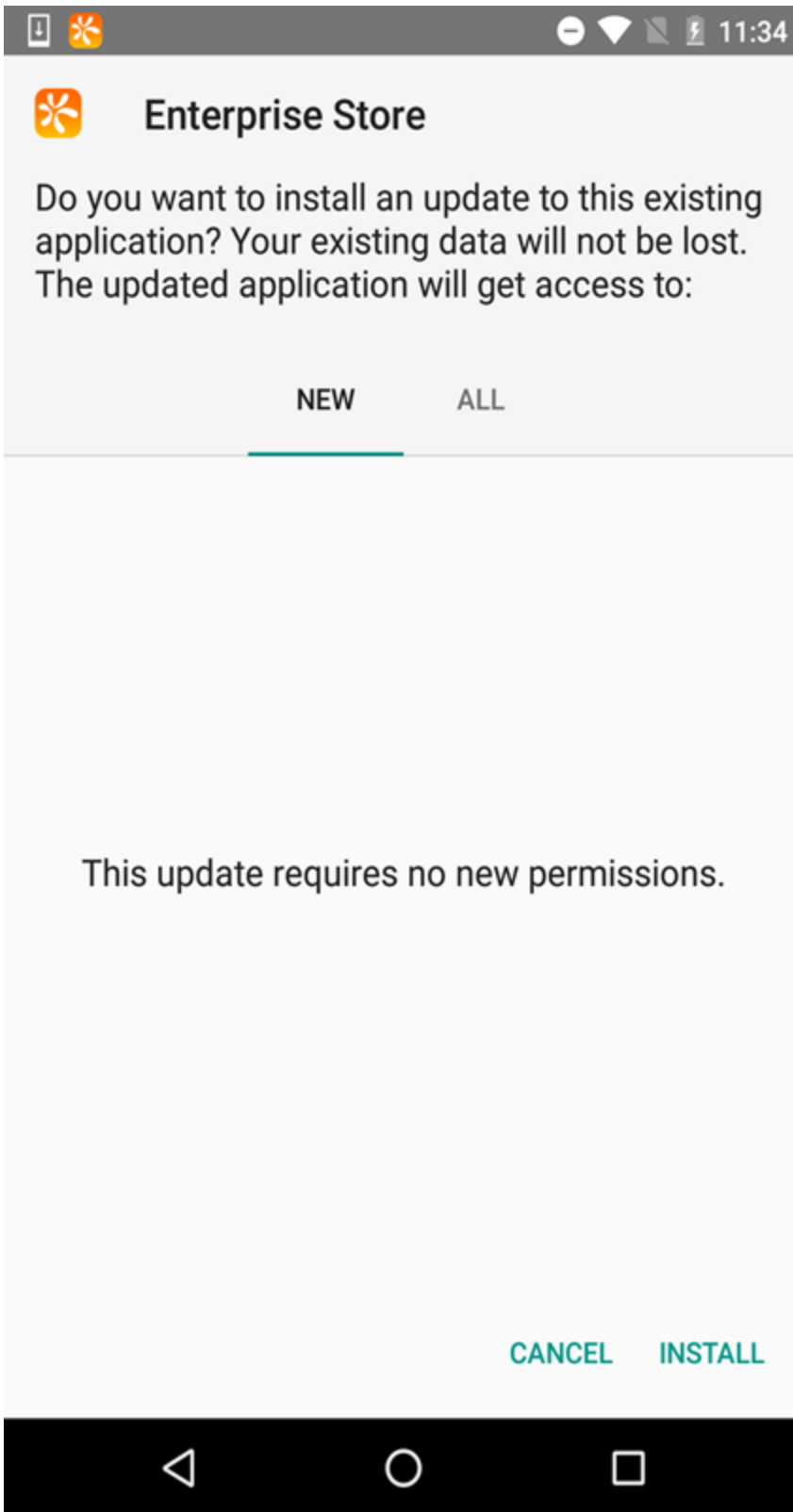


Once you click **Ok**, the page redirects to the download link of the enterprise store.



Click **Download**. The app downloads.

Open the downloaded apk file. An Install screen appears.



Click **Install**. Screen goes back to the home page and the enterprise store is installed.

8.3.11.3 Upgrade Enterprise Store in Windows

When you have an update available for your enterprise store in iOS, you will receive a push message.

Once you log in to the device, a mandatory upgrade message

Click Ok. An Install message appears.

Click Install. Screen goes back to the home page and the enterprise store is installed.

9. Device Management

The only purpose of this section is to show the list of devices associated with Users.

The Admin can get a limited view of devices compared to a complete EMM deployment.

9.1 Managing Devices

Managing devices includes:

- [Device](#)

9.2 Devices

The primary purpose of Devices page is to provide all the information about devices and perform different activities to manage them efficiently.

From the **Device Management** section, click the **Devices** from the left panel. The Devices page appears with a list of theregistered devices. The view displays a list of all the devices along with other details. You can search the devices based on each column and also sort on each column.

The Devices list view displays the following columns:

| Columns | Description |
|--------------|---|
| Device Name | <p>Displays the device name with the domain name as given to the device by the system. The device list can be sorted on the following:</p> <ul style="list-style-type: none"> • Device name • IMEI • Serial number • SIM ID <p>You can also search for a device based on the device name, IMEI number, serial number, and SIM ID.</p> |
| Status | <p>Displays the current status of the device. Devices Statuses are as follows:</p> <ul style="list-style-type: none"> • Enrolled: The Device is registered with EMM Console. • Deactivated: The Device status is changed from active to inactive. |
| Device Owner | Displays the name of User with whom the Device is registered. |

| Columns | Description |
|------------------------------|---|
| Ownership | Displays the ownership of the device. Options are Corporate, Employee, and Shared. |
| OS | Displays the Operating System version present on the device. |
| Last Check-in | Time Stamp of the last time the device communicated with the EMM Server. |
| Date Enrolled of First Login | Displays when the device was enrolled to EMM Console, for example, Today, Yesterday or Last 7 Days. |
| Action | Displays the action taken on the device. |

9.2.1 Device Statuses

Displays the current status of the device are as follows:

- **Enrolled:** The Device is registered with EMM Console and is active.
- **Deactivated:** It is recommended to assign this status to indicate that the device is not enrolled to EMM and can be enrolled by another user.

9.2.2 Deleting Device List Entries

An administrator can select one or more entries in the Device List and delete those entries. Those entries will no longer appear on the Device List.

To delete Device List entries, follow these steps:

1. Select the check box next to the specified Device Name.

The **Delete** button is active only if the Device Status is set to one of the statuses below:

- Control Removed
- Deactivated
- Device Lost
- Retired

For any other status, the Delete button is not active:

2. Click the **Delete** button. The system displays the following message:

The chosen device(s) shall be removed from the device list. Are you sure you want to do this?

3. Click **Yes** to confirm. The selected entry removed.

Note: Suspended devices are always shown in the Device List but cannot be deleted.

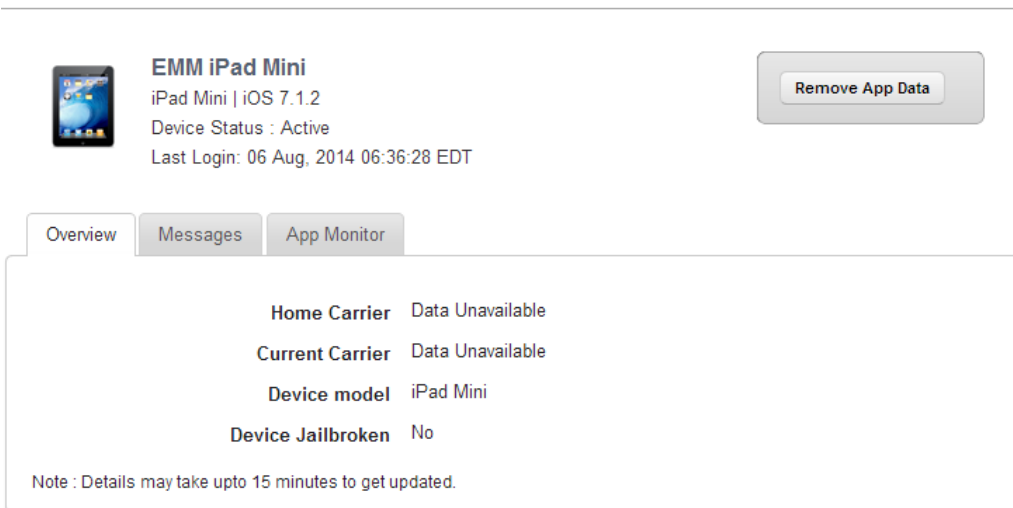
Important: When an enrolled device is purged from the **Admin Console** and the device gets the notification as purged; and a user tries to login the device in offline mode, the user can still login and access to the Launchpad still works. Therefore, whenever the device enrolment status changes, you need to login again to update the status on the device. The scenario also applies to **Enterprise Wipe, Purge, and Blocked Devices**.

9.3 Device Details

The primary purpose of the Device Details page is to display complete information of a device and manage the device through various actions available.

Device Details

[Device List](#) > Device Details



EMM iPad Mini
iPad Mini | iOS 7.1.2
Device Status : Active
Last Login: 06 Aug, 2014 06:36:28 EDT

Remove App Data

Overview Messages App Monitor

Home Carrier Data Unavailable
Current Carrier Data Unavailable
Device model iPad Mini
Device Jailbroken No

Note : Details may take upto 15 minutes to get updated.

The Device Details Page includes the following screen elements:

- **Home Carrier:** Displays the carrier details from whom the phone was purchased.
- **Current Carrier:** Displays the name of the current carrier network the device is on.
- **Device Model:** Displays the model details of the device.
- **Device Jailbroken:** Displays whether the device is jail broken or not.

Note: For iOS, even after the SIM card is removed from a device, the Home Carrier field and the Current Carrier field in the Device Details page under Overview tab display the existing carrier details.

The Device Details Page content is divided into the following sections.

- [Device Details Page Tabs](#)
- [Device Details page Actions](#)

9.3.1 Device Details Page Tabs

Device details page displays the following tabs:

- [Overview](#)
- [Messages](#)
- [App Monitor](#)

9.3.1.1 Overview

By default Overview tab is set to active. This tab displays the various attributes of the device. You can update the ownership details only.

Overview for iOS

- **Home Carrier:** Displays the carrier details from whom the phone was purchased.
- **Current Carrier:** Displays the name of the current carrier network the device is on.
- **Device Model:** Displays the model details of the device.
- **Device Jailbroken:** Displays whether the device is jail broken or not.

Overview for Android

**EMM Nexus 5**

Nexus 5 | Android 4.4.4

Device Status : Active

IMEI: 353490061504094

Last Login: 06 Aug, 2014 06:34:51 EDT

[Remove App Data](#)

Overview

Messages

App Monitor

| | |
|--------------------------|---------------------|
| Manufacturer | Lge |
| Home Carrier | Data Unavailable |
| Current Carrier | Data Unavailable |
| Serial Number | Data Unavailable |
| IMEI Number | 353490061504094 |
| SIM ID | Data Unavailable |
| Storage Used | 0.50 GB / 12.55 GB |
| Storage Available | 12.05 GB / 12.55 GB |
| Device Rooted | No |
| Screen Size | Data Unavailable |

Note : Details may take upto 15 minutes to get updated.

- **Manufacturer:** Displays the details of the manufacturer of the device.
- **Home Carrier:** Displays the carrier details from whom the phone was purchased.
- **Current Carrier:** Displays the name of the current carrier network the device is on.
- **Serial Number:** Displays the serial number of the device.
- **IMEI Number:** Displays the IMEI number of the device.
- **SIM ID:** Displays the SIM ID.
- **Storage Used:** Displays the amount of storage used by the device.
- **Storage Available:** Displays the amount of storage available.

- **Device Rooted:** Displays whether device root access is enabled.
- **Screen Size:** Displays the screen size of the device.

Device Details Purge

Devices > Device Details



Bipin Lumia 630

Lumia 630 | Windows Phone 8.1
 Device Status : Enrolled
 UDID: 3F86E331-91BD-5787-9385-A30B7EE986BE
 Last sync: 11 Nov, 2014 11:36:03 EST

Lock Device Reset Passcode
Ring Device Wipe Actions
Remove App Data Block Email
Unblock Email

- Overview
- Messages
- Locate
- App Monitor
- EMM Info
- Device Sets

| | |
|-------------------------------------|--|
| Ownership | Employee ▼ |
| Device Model | Nokia Lumia 630 |
| Platform | Windows Phone 8.x |
| OEM | Nokia |
| Firmware Version | 01061.00066.14235.36002 |
| OS Software Version | Windows Phone 8.1 |
| Processor Type | X86 |
| Processor Architecture | Arm |
| Local Time | 11 Nov, 2014 16:13:15 IST |
| Screen Size | 480x800 |
| Carrier | airtel |
| Carrier (SIM2) | Data Unavailable |
| WLAN MAC Address | D4-8F-33-B6-23-6B |
| Current Language | English |
| Phone Number | Data Unavailable 🔒 8.1+ |
| Phone Number (SIM2) | Data Unavailable 🔒 8.1+ |
| Device name | Windows Phone 🔒 8.1+ |
| Device Roaming Status | Non Roaming 🔒 8.1+ |
| Device Roaming Status (SIM2) | Data Unavailable 🔒 8.1+ |
| IMEI Number | 354271067826189 🔒 8.1+ |
| MDM Policy | Data Unavailable |

Note : Details may take upto 15 minutes to get updated.

- Save & Exit
- Save & Continue
- Cancel

- **Ownership:** Displays the ownership of the device. Available options are Corporate, Employee, and Shared.
- **Device Model:** Displays the details of device model.
- **Platform:** Displays platform details of the device.
- **OEM:** Displays OEM details of the device.
- **Firmware Version:** Displays the firmware version of the device.
- **OS Software Version:** Displays the operating system software version of the device.
- **Processor Type:** Displays the details of the device processor.
- **Processor Architecture:** Displays the details of the device processor architecture.
- **Local Time:** Displays the device local time.
- **Screen Size:** Displays details of screen size of the device.
- **Carrier:** Displays the name of the carrier network the device is on.
- **Carrier (SIM2):** Displays the name of the current carrier network the device is on.
- **WLAN MAC Address:** Displays WLAN MAC address of the device.
- **Current Language:** Displays the device's current language.
- **Phone Number:** Displays the phone number of the device.
- **Phone Number (SIM2):** Displays the phone number of the second sim card of the device.
- **Device Name:** Displays the name of the device.
- **Device Roaming Status:** Displays details on whether the device is on roaming or not.
- **Device Roaming Status (SIM2):** Displays details on whether the device's second sim card is on roaming or not.
- **IMEI Number:** Displays the IMEI number of the device.

- **MDM Policy:** Displays details of MDM policy applied on the device.

Processor

| | |
|-------------------------------------|------------------|
| Processor Architecture | Data Unavailable |
| Family | Data Unavailable |
| Number of Logical Processors | Data Unavailable |

Systems

| | |
|---|------------------|
| Bluetooth | Data Unavailable |
| Wi-Fi | Data Unavailable |
| Sync to personal OneDrive | Data Unavailable |
| Sync Over Metered Network | Data Unavailable |
| Workfolders Autoprovisioning on Device | Data Unavailable |
| Smart Screen | Data Unavailable |

System Status

| | |
|------------------------------------|------------------|
| Firewall Status | Data Unavailable |
| Auto Update Status | Data Unavailable |
| Anti Virus Status | Data Unavailable |
| Anti Virus Signature Status | Data Unavailable |

Battery

| | |
|--------------------------------------|------------------|
| Battery Availability | Data Unavailable |
| Battery Status | Data Unavailable |
| Chemistry(Composition) | Data Unavailable |
| Design Capacity | Data Unavailable |
| Full Charge Capacity | Data Unavailable |
| Estimated Charge Remaining | Data Unavailable |
| Estimated Run Time | Data Unavailable |
| Power Management Supported | Data Unavailable |
| Power Management Capabilities | Data Unavailable |
| Time to Full Charge | Data Unavailable |
| Expected Battery life | Data Unavailable |
| Max Recharge Time | Data Unavailable |

Note : Details may take upto 15 minutes to get updated.

Save & Exit

Save & Continue

Cancel

- **Ownership:** Displays details of ownership of the device. Options are Corporate, Employee, and Shared.
- **MDM Policy:** Displays details of MDM policy applied on the device.
- **MAC Address:** Displays the MAC address of the network adapter.
- **Manufacturer:** Displays details of the manufacturer of the device.
- **Device Model:** Displays device model details.
- **Total Physical Memory:** Displays details of total physical memory of the device.

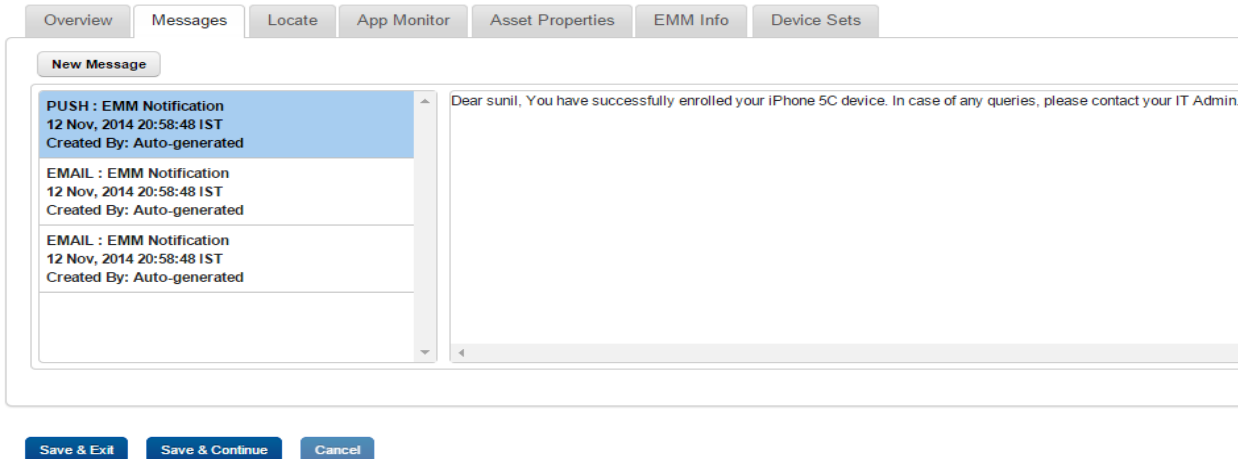
- **Username:** Displays username of the device user.
- **DomainRole:** Displays details of domain role of the device.
- **Current time Zone:** Displays the local time zone details of the device.
- **HDD Manufacturer:** Displays details of the HDD manufacturer.
- **HDD Availability:** Displays details of HDD availability.
- **Processor Architecture:** Displays details of processor architecture.
- **Family:** Displays details of the processor family.
- **Number of Logical Processors:** Displays details of logical processors available on the device.
- **Bluetooth enabled:** Displays details on whether bluetooth is enabled.
- **Wi-Fi enabled:** Displays details on whether Wi-Fi is enabled.
- **Sync to personal OneDrive:** Displays details on whether the device is synced with personal OneDrive account.
- **Sync Over Metered Network:** Displays details about whether the device can sync over metered network.
- **Workfolders Autoprovisioning on Device:** Displays whether the device has auto-provisioning for work folders.
- **Smart Screen:** Displays details about smart screen if the device has a smart screen.
- **Firewall Status:** Displays details on the status of the firewall.
- **Auto Update Status:** Displays details on auto update settings.
- **Anti Virus Status:** Displays details on anti virus available on the device.
- **Anti Virus Signature Status:** Displays details on the status of anti virus signature.
- **Battery Availability:** Displays details on battery availability.

- **Battery Status:** Displays details on status of the battery.
- **Chemistry(Composition):** Displays details of the chemical composition of the battery.
- **Design Capacity:** Displays details about the design capacity of the battery.
- **Full Charge Capacity:** Displays details on the full charge capacity of the battery.
- **Estimated Charge Remaining:** Displays details of the remaining charge on the battery.
- **Estimated Run Time:** Displays details on how long the battery can run.
- **Power Management Supported:** Displays details of power management if power management is supported.
- **Power Management Capabilities:** Displays details of power management capabilities.
- **Time to Full Charge:** Displays the time needed to fully charge of the battery.
- **Expected Battery life:** Displays details on the expected battery life of the device.
- **Max Recharge Time:** Displays details on the maximum amount of time needed to recharge the battery of the device.

9.3.1.2 Messages

This option is used to send a message to a device user. The administrator can send a message to a Device User for various reasons, for example,

- Inform the user about a new requirement or development.
- Request the user to take an immediate action, for example, any compliance issue.
- Inform the user about completion of certain tasks.
- The Device Users receive the message in the mode specified and can view the same.



To compose a message, follow these steps:

1. Click the **New Message** button to open the **Compose Message** window. Enter the following details:

2. **Send As:** By default this option is set to **Email**. You can modify it to **Push Notification**.

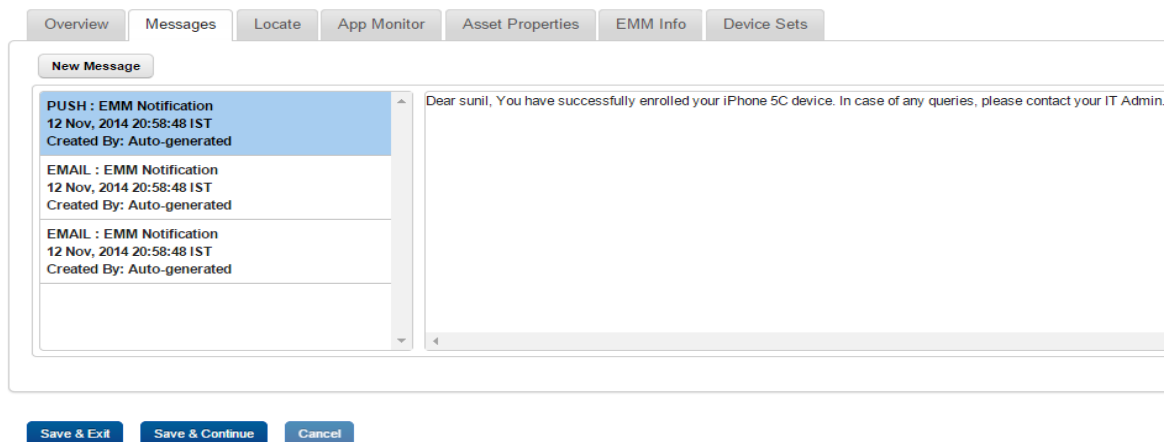
3. **Compose from Template:** Select the required option from the drop-down menu.

To automate the work-flow process, you create message templates under Device Settings > Message Templates section. You can access these messages in Compose Message window through Compose from Template dropdown list.

4. **Personalization Attributes:** Select the required attribute from the dropdown list. These details are populated through Active Directory.

The Personalized Attributes are predefined and system displays the related details as per the selected attributes. For example, if you select Device OS, Device Name, and the Device Model No from the dropdown list. The respective details are picked up from the device and appended in the sent message.

5. Click the **Add** button. The details appear in the Message Box.
6. Click the **Send** button to submit the message. In the confirmation message (Send Message - Success) that appears, click OK to continue.

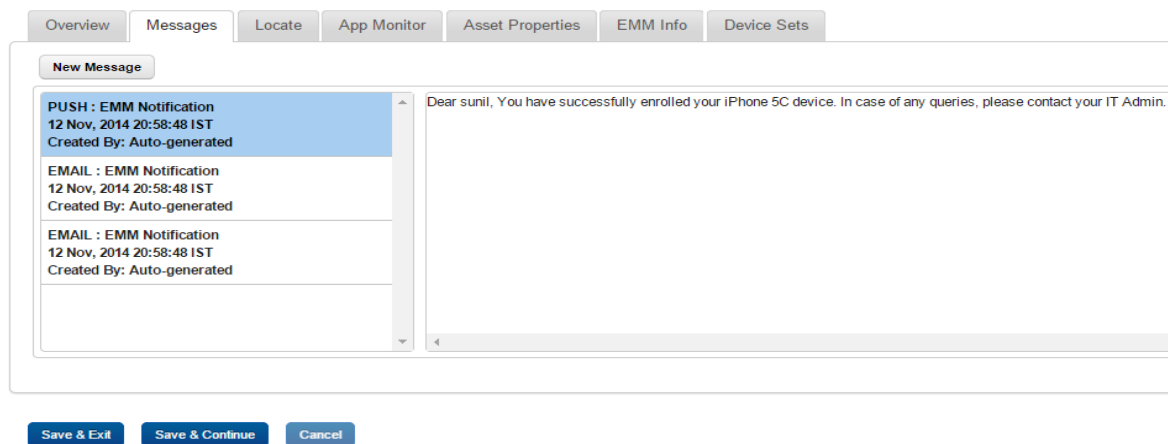


The message appears in the message window

7. **Personalization Attributes:** Select the required attribute from the dropdown list. These details are populated through Active Directory.

The Personalized Attributes are predefined and system displays the related details as per the selected attributes. For example, if you select Device OS, Device Name, and the Device Model No from the dropdown list. The respective details are picked up from the device and appended in the sent message.

8. Click the **Add** button. The details appear in the Message Box.
9. Click the **Send** button to submit the message. In the confirmation message (Send Message - Success) that appears, click **OK** to continue.



The message appears in the message window.

9.3.1.3 Locate

The Locate Tab displays the location details. You may wish to know the location of a device under several situations. For example,

- The device is out of compliance and you wish to take some action against the same.
- You receive an alert on the device.
- User is traveling.
- User is absent without notice for a while.

Last Known Location

A.  H-08
 03:27 IST
 17.447296 78.371079
 H-08, Rolling Hills, Gachibowli, Hyderabad,
 Andhra Pradesh 500081, India

Last Five Locations [map all](#)

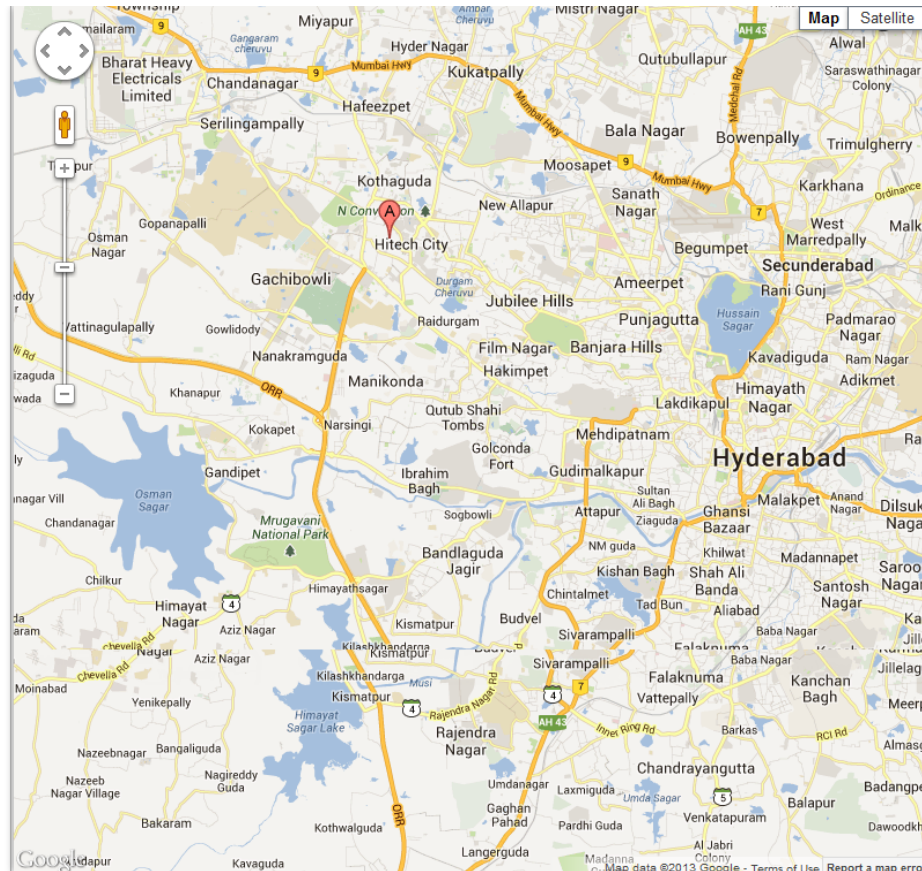
B. H-08, Rolling Hills, Gachibowli, Hyderabad,
 Andhra Pradesh 500081, India
 03:27 IST
 17.447393 78.371048

C. H-08, Rolling Hills, Gachibowli, Hyderabad,
 Andhra Pradesh 500081, India
 03:20 IST
 17.447296 78.371080

D. H-08, Rolling Hills, Gachibowli, Hyderabad,
 Andhra Pradesh 500081, India
 03:08 IST
 17.44713370689884 78.37106321014312

E. H-08, Rolling Hills, Gachibowli, Hyderabad,
 Andhra Pradesh 500081, India
 10:00 IST

F. H-08, Rolling Hills, Gachibowli, Hyderabad,
 Andhra Pradesh 500081, India
 09:56 IST
 17.44713370689884 78.37106321014312



You can view the most recently polled location of the device both in terms of coordinates as well as the address as indicated by the used maps service.

You can also view the last 5 locations of the device as per the location samples collected. The system displays the following location information about the device:

- Current location
 - Location Address (as provided by the maps software used)
 - Time of Polling (Time specified in UTC)
 - Map (with pinned location) with latitude and longitude details

- Past 5 locations
 - Location Pin Name
 - Location Addresses
 - Time of Polling

You can zoom in and zoom out as required.

Important: If location is turned off on device, then portal does not display the map with last five locations.

Note: If you are using a free Google Maps license, when the limit is reached you will see an error - 'Geo coder failed due to:OVER_QUERY_LIMIT'. In such cases it is recommended to move to a business license.

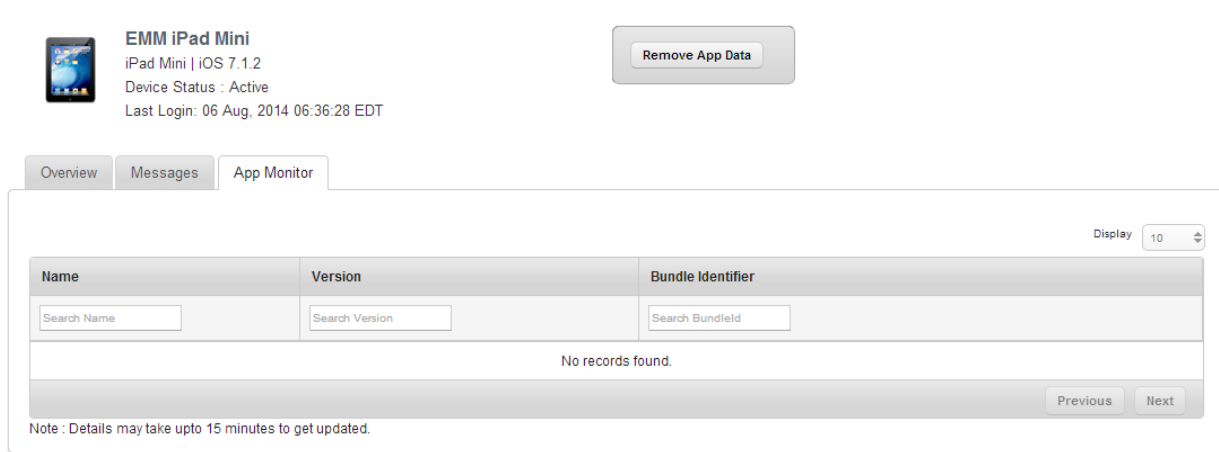
9.3.1.4 App Monitor

The App Monitor displays the installed apps on a device. It does not display default apps that are installed with OS.

- **Installed Apps:** Installed Apps section displays all apps that are installed on the device. Details of installed apps and app details vary based on the operating system of the device. You can find more details on it in the sections below specific for each OS.
- **Targeted Apps:** This section displays all apps targeted to a device but not installed on the device.

There are types of Apps shown.

App Monitor for iOS



EMM iPad Mini
 iPad Mini | iOS 7.1.2
 Device Status : Active
 Last Login: 06 Aug, 2014 06:36:28 EDT

Remove App Data

Overview Messages App Monitor

Display 10

| Name | Version | Bundle Identifier |
|--|---|--|
| <input type="text" value="Search Name"/> | <input type="text" value="Search Version"/> | <input type="text" value="Search BundleId"/> |
| No records found. | | |
| | | Previous Next |

Note : Details may take upto 15 minutes to get updated.

The App Monitor list view for iOS has the following details:

- **Name:** Displays the Name of the application.
- **Version:** Displays the Version of the application.
- **Bundle Identifier:** Displays the bundle ID of the application.

Note: In the App Monitor tab for iOS, Publisher has been replaced with Bundle Identifier.

App Monitor for Android

You can search a desired app through search filters based on all grid columns. You can apply a single or a combination of search filters to define the search criteria and get the refined outcome.

Device Details

[Device List](#) > Device Details

EMM Nexus 5
Nexus 5 | Android 4.4.4
Device Status : Active
IMEI: 353490061504094
Last Login: 06 Aug, 2014 06:34:51 EDT

[Remove App Data](#)

Overview Messages **App Monitor**

Display 10

| Name | Version | Package Name |
|--|---|--|
| <input type="text" value="Search Name"/> | <input type="text" value="Search Version"/> | <input type="text" value="Search Package Name"/> |
| No records found. | | |

[Previous](#) [Next](#)

Note : Details may take upto 15 minutes to get updated.

The App Monitor list view for Android SAFE devices has the following details:

To search for an app, follow these steps:

1. **Name:** Displays the Name of the application.
2. **Version:** Displays the Name of the application.
3. **Package Name:** Displays the package name of the application.

9.3.2 Device Details Page Actions

You can perform the following activities from Device List page.

- [Searching for Devices](#)
- [Updating Device Details](#)
- [Locking a Device](#)
- [Remove App Data](#)

9.3.2.1 Searching for Devices

You search for devices through search filters based on all grid columns. You can apply a single or a combination of search filters to define the search criteria and get the refined outcome. To search a device, follow these steps:

| | Device Name ▼ | Device Owner | OS | Last Login | Date of First Login | Status |
|--------------------------|---|--|--|-------------------------------|-------------------------------|---|
| | <input type="text" value="Search Device Name"/> | <input type="text" value="Search Device Owr"/> | <input type="text" value="Search OS"/> | All ▾ | All ▾ | |
| <input type="checkbox"/> | EMM iPad Mini | EMM Admin | 🍏 iOS 7.1.2 | 06 Aug, 2014 06:36:28 E DT | 06 Aug, 2014 06:36:28 E DT | <input type="button" value="Deactivate"/> |
| <input type="checkbox"/> | EMM Nexus 5 | EMM Admin | 🤖 Android 4.4.4 | 06 Aug, 2014 06:34:51 E DT | 06 Aug, 2014 06:34:51 E DT | <input type="button" value="Deactivate"/> |

1. Enter or select details for the following search filters:
 - a. **Device Name:** Enter partial or a complete device name in the **Search Device Name** text field.
 - b. **Status:** Select the desired option from the drop-down list.
 - c. **Device Owner:** Enter partial or a complete owner name in the **Search Device Owner** text field.
 - d. **Ownership:** Select the required category from the dropdown list.
 - e. **OS:** Enter desired operating system version in the **Search OS** text field.
 - f. **Last Log in:** Shows several options to shortlist the Last Log in by.
 - g. **Date of First Login:** This is the date of registration of the device.

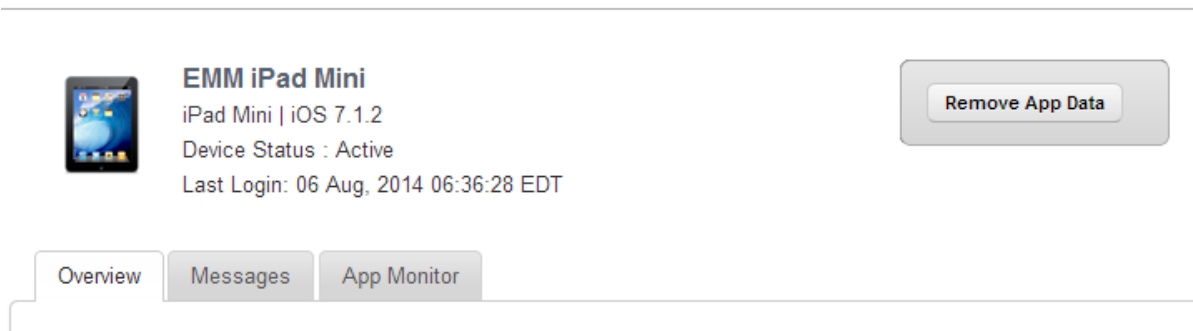
2. According to your search filter criteria, the list view is updated with respective device details. By default, the list view displays ten devices according to Display settings, which you can modify through Display dropdown list. You can also scroll the list view through **Previous** and the **Next** buttons.

9.3.2.2 Remove App Data

Remove App Data is only applicable to Enterprise Apps that are wrapped-signed and pushed through EMM and not for side-loaded apps. This action is performed to remove all the data from the apps. This action is performed by an enterprise store to retain the apps but remove the app data to retain safety.

Device Details

[Device List](#) > Device Details



EMM iPad Mini
iPad Mini | iOS 7.1.2
Device Status : Active
Last Login: 06 Aug, 2014 06:36:28 EDT

Remove App Data

Overview Messages App Monitor

To remove the data from the apps, follow these steps:

1. Click the required device in the list view.

The **Device Details** page appears.

2. Click the **Remove App data** button.

The System displays the warning message (**Remove App Data**) asking the user, if really wishes to remove all the corporate data from the device.

3. Click the **Remove** button to remove the app data. In the confirmation message (Remove App Data) that appears, click **OK** to return to the page.

Note: For Windows Phone 8.x devices, the remove app data policy will not work if the app is in use. The policy command will apply when the app is closed and relaunched.

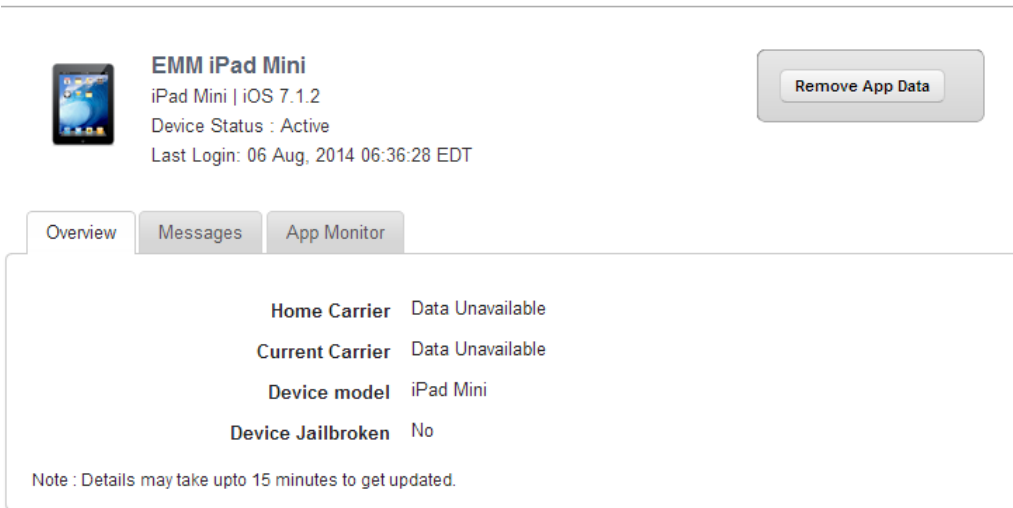
Note: If this is applied for non-supervised devices, the command will not execute.

9.3.3 Device Details

The primary purpose of the Device Details page is to display complete information of a device and manage the device through various actions available.

Device Details

[Device List](#) > Device Details



EMM iPad Mini
iPad Mini | iOS 7.1.2
Device Status : Active
Last Login: 06 Aug, 2014 06:36:28 EDT

Remove App Data

Overview Messages App Monitor

| | |
|-------------------|------------------|
| Home Carrier | Data Unavailable |
| Current Carrier | Data Unavailable |
| Device model | iPad Mini |
| Device Jailbroken | No |

Note : Details may take upto 15 minutes to get updated.

The Device Details Page includes the following screen elements:

- **Home Carrier:** Displays the carrier details from whom the phone was purchased.
- **Current Carrier:** Displays the name of the current carrier network the device is on.
- **Device Model:** Displays the model details of the device.
- **Device Jailbroken:** Displays whether the device is jail broken or not.

Note: For iOS, even after the SIM card is removed from a device, the Home Carrier field and the Current Carrier field in the Device Details page under Overview tab display the existing carrier details.

The Device Details Page content is divided into the following sections.

- [Device Details Page Tabs](#)
- [Device Details page Actions](#)

9.3.3.1 Device Details Page Tabs

Device details page displays the following tabs:

- [Overview](#)
- [Messages](#)
- [App Monitor](#)

Overview

By default Overview tab is set to active. This tab displays the various attributes of the device. You can update the ownership details only.

Overview for iOS

- **Home Carrier:** Displays the carrier details from whom the phone was purchased.
- **Current Carrier:** Displays the name of the current carrier network the device is on.
- **Device Model:** Displays the model details of the device.
- **Device Jailbroken:** Displays whether the device is jail broken or not.

Overview for Android

**EMM Nexus 5**

Nexus 5 | Android 4.4.4

Device Status : Active

IMEI: 353490061504094

Last Login: 06 Aug, 2014 06:34:51 EDT

[Remove App Data](#)

Overview

Messages

App Monitor

| | |
|--------------------------|---------------------|
| Manufacturer | Lge |
| Home Carrier | Data Unavailable |
| Current Carrier | Data Unavailable |
| Serial Number | Data Unavailable |
| IMEI Number | 353490061504094 |
| SIM ID | Data Unavailable |
| Storage Used | 0.50 GB / 12.55 GB |
| Storage Available | 12.05 GB / 12.55 GB |
| Device Rooted | No |
| Screen Size | Data Unavailable |

Note : Details may take upto 15 minutes to get updated.

- **Manufacturer:** Displays the details of the manufacturer of the device.
- **Home Carrier:** Displays the carrier details from whom the phone was purchased.
- **Current Carrier:** Displays the name of the current carrier network the device is on.
- **Serial Number:** Displays the serial number of the device.
- **IMEI Number:** Displays the IMEI number of the device.
- **SIM ID:** Displays the SIM ID.
- **Storage Used:** Displays the amount of storage used by the device.
- **Storage Available:** Displays the amount of storage available.

- **Device Rooted:** Displays whether device root access is enabled.
- **Screen Size:** Displays the screen size of the device.

Device Details Purge

Devices > Device Details



Bipin Lumia 630

Lumia 630 | Windows Phone 8.1
 Device Status : Enrolled
 UDID: 3F86E331-91BD-5787-9385-A30B7EE986BE
 Last sync: 11 Nov, 2014 11:36:03 EST

Lock Device Reset Passcode
Ring Device Wipe Actions
Remove App Data Block Email
Unblock Email

- Overview
- Messages
- Locate
- App Monitor
- EMM Info
- Device Sets

| | |
|-------------------------------------|--|
| Ownership | Employee ▼ |
| Device Model | Nokia Lumia 630 |
| Platform | Windows Phone 8.x |
| OEM | Nokia |
| Firmware Version | 01061.00066.14235.36002 |
| OS Software Version | Windows Phone 8.1 |
| Processor Type | X86 |
| Processor Architecture | Arm |
| Local Time | 11 Nov, 2014 16:13:15 IST |
| Screen Size | 480x800 |
| Carrier | airtel |
| Carrier (SIM2) | Data Unavailable |
| WLAN MAC Address | D4-8F-33-B6-23-6B |
| Current Language | English |
| Phone Number | Data Unavailable 🔒 8.1+ |
| Phone Number (SIM2) | Data Unavailable 🔒 8.1+ |
| Device name | Windows Phone 🔒 8.1+ |
| Device Roaming Status | Non Roaming 🔒 8.1+ |
| Device Roaming Status (SIM2) | Data Unavailable 🔒 8.1+ |
| IMEI Number | 354271067826189 🔒 8.1+ |
| MDM Policy | Data Unavailable |

Note : Details may take upto 15 minutes to get updated.

- Save & Exit
- Save & Continue
- Cancel

- **Ownership:** Displays the ownership of the device. Available options are Corporate, Employee, and Shared.
- **Device Model:** Displays the details of device model.
- **Platform:** Displays platform details of the device.
- **OEM:** Displays OEM details of the device.
- **Firmware Version:** Displays the firmware version of the device.
- **OS Software Version:** Displays the operating system software version of the device.
- **Processor Type:** Displays the details of the device processor.
- **Processor Architecture:** Displays the details of the device processor architecture.
- **Local Time:** Displays the device local time.
- **Screen Size:** Displays details of screen size of the device.
- **Carrier:** Displays the name of the carrier network the device is on.
- **Carrier (SIM2):** Displays the name of the current carrier network the device is on.
- **WLAN MAC Address:** Displays WLAN MAC address of the device.
- **Current Language:** Displays the device's current language.
- **Phone Number:** Displays the phone number of the device.
- **Phone Number (SIM2):** Displays the phone number of the second sim card of the device.
- **Device Name:** Displays the name of the device.
- **Device Roaming Status:** Displays details on whether the device is on roaming or not.
- **Device Roaming Status (SIM2):** Displays details on whether the device's second sim card is on roaming or not.
- **IMEI Number:** Displays the IMEI number of the device.

- **MDM Policy:** Displays details of MDM policy applied on the device.

Processor

| | |
|-------------------------------------|------------------|
| Processor Architecture | Data Unavailable |
| Family | Data Unavailable |
| Number of Logical Processors | Data Unavailable |

Systems

| | |
|---|------------------|
| Bluetooth | Data Unavailable |
| Wi-Fi | Data Unavailable |
| Sync to personal OneDrive | Data Unavailable |
| Sync Over Metered Network | Data Unavailable |
| Workfolders Autoprovisioning on Device | Data Unavailable |
| Smart Screen | Data Unavailable |

System Status

| | |
|------------------------------------|------------------|
| Firewall Status | Data Unavailable |
| Auto Update Status | Data Unavailable |
| Anti Virus Status | Data Unavailable |
| Anti Virus Signature Status | Data Unavailable |

Battery

| | |
|--------------------------------------|------------------|
| Battery Availability | Data Unavailable |
| Battery Status | Data Unavailable |
| Chemistry(Composition) | Data Unavailable |
| Design Capacity | Data Unavailable |
| Full Charge Capacity | Data Unavailable |
| Estimated Charge Remaining | Data Unavailable |
| Estimated Run Time | Data Unavailable |
| Power Management Supported | Data Unavailable |
| Power Management Capabilities | Data Unavailable |
| Time to Full Charge | Data Unavailable |
| Expected Battery life | Data Unavailable |
| Max Recharge Time | Data Unavailable |

Note : Details may take upto 15 minutes to get updated.

Save & Exit

Save & Continue

Cancel

- **Ownership**: Displays details of ownership of the device. Options are Corporate, Employee, and Shared.
- **MDM Policy**: Displays details of MDM policy applied on the device.
- **MAC Address**: Displays the MAC address of the network adapter.
- **Manufacturer**: Displays details of the manufacturer of the device.
- **Device Model**: Displays device model details.
- **Total Physical Memory**: Displays details of total physical memory of the device.

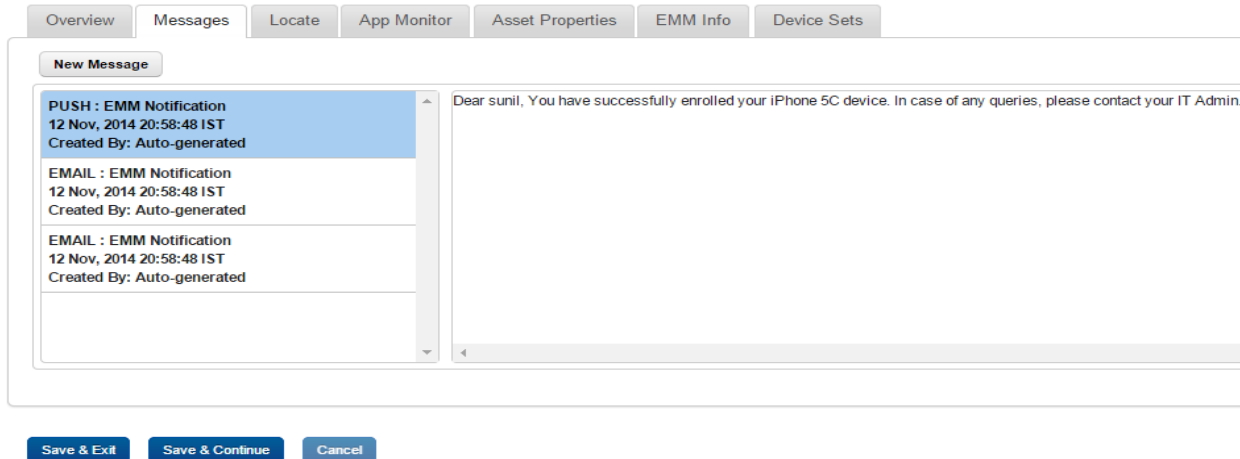
- **Username:** Displays username of the device user.
- **DomainRole:** Displays details of domain role of the device.
- **Current time Zone:** Displays the local time zone details of the device.
- **HDD Manufacturer:** Displays details of the HDD manufacturer.
- **HDD Availability:** Displays details of HDD availability.
- **Processor Architecture:** Displays details of processor architecture.
- **Family:** Displays details of the processor family.
- **Number of Logical Processors:** Displays details of logical processors available on the device.
- **Bluetooth enabled:** Displays details on whether bluetooth is enabled.
- **Wi-Fi enabled:** Displays details on whether Wi-Fi is enabled.
- **Sync to personal OneDrive:** Displays details on whether the device is synced with personal OneDrive account.
- **Sync Over Metered Network:** Displays details about whether the device can sync over metered network.
- **Workfolders Autoprovisioning on Device:** Displays whether the device has auto-provisioning for work folders.
- **Smart Screen:** Displays details about smart screen if the device has a smart screen.
- **Firewall Status:** Displays details on the status of the firewall.
- **Auto Update Status:** Displays details on auto update settings.
- **Anti Virus Status:** Displays details on anti virus available on the device.
- **Anti Virus Signature Status:** Displays details on the status of anti virus signature.
- **Battery Availability:** Displays details on battery availability.

- **Battery Status:** Displays details on status of the battery.
- **Chemistry(Composition):** Displays details of the chemical composition of the battery.
- **Design Capacity:** Displays details about the design capacity of the battery.
- **Full Charge Capacity:** Displays details on the full charge capacity of the battery.
- **Estimated Charge Remaining:** Displays details of the remaining charge on the battery.
- **Estimated Run Time:** Displays details on how long the battery can run.
- **Power Management Supported:** Displays details of power management if power management is supported.
- **Power Management Capabilities:** Displays details of power management capabilities.
- **Time to Full Charge:** Displays the time needed to fully charge of the battery.
- **Expected Battery life:** Displays details on the expected battery life of the device.
- **Max Recharge Time:** Displays details on the maximum amount of time needed to recharge the battery of the device.

Messages

This option is used to send a message to a device user. The administrator can send a message to a Device User for various reasons, for example,

- Inform the user about a new requirement or development.
- Request the user to take an immediate action, for example, any compliance issue.
- Inform the user about completion of certain tasks.
- The Device Users receive the message in the mode specified and can view the same.



To compose a message, follow these steps:

1. Click the **New Message** button to open the **Compose Message** window. Enter the following details:

2. **Send As:** By default this option is set to **Email**. You can modify it to **Push Notification**.

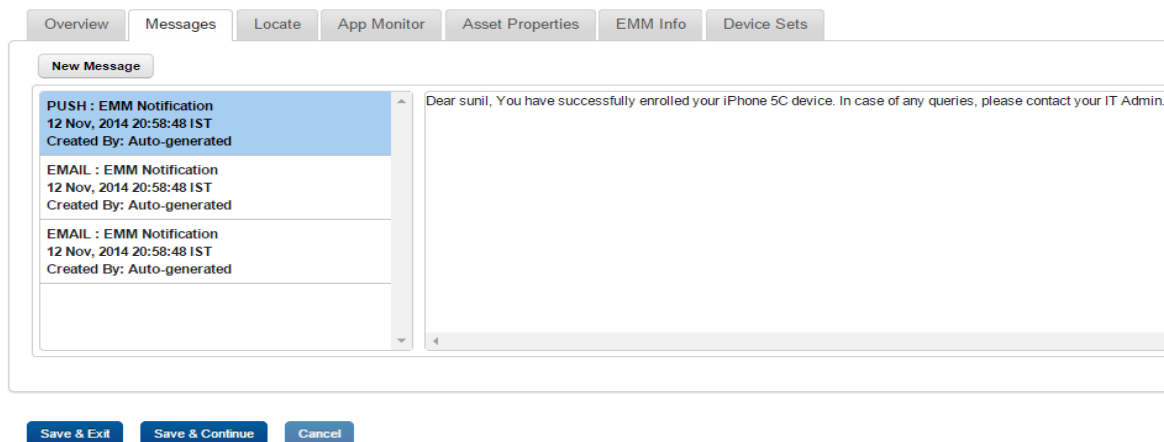
3. **Compose from Template:** Select the required option from the drop-down menu.

To automate the work-flow process, you create message templates under Device Settings > Message Templates section. You can access these messages in Compose Message window through Compose from Template dropdown list.

4. **Personalization Attributes:** Select the required attribute from the dropdown list. These details are populated through Active Directory.

The Personalized Attributes are predefined and system displays the related details as per the selected attributes. For example, if you select Device OS, Device Name, and the Device Model No from the dropdown list. The respective details are picked up from the device and appended in the sent message.

5. Click the **Add** button. The details appear in the Message Box.
6. Click the **Send** button to submit the message. In the confirmation message (Send Message - Success) that appears, click OK to continue.

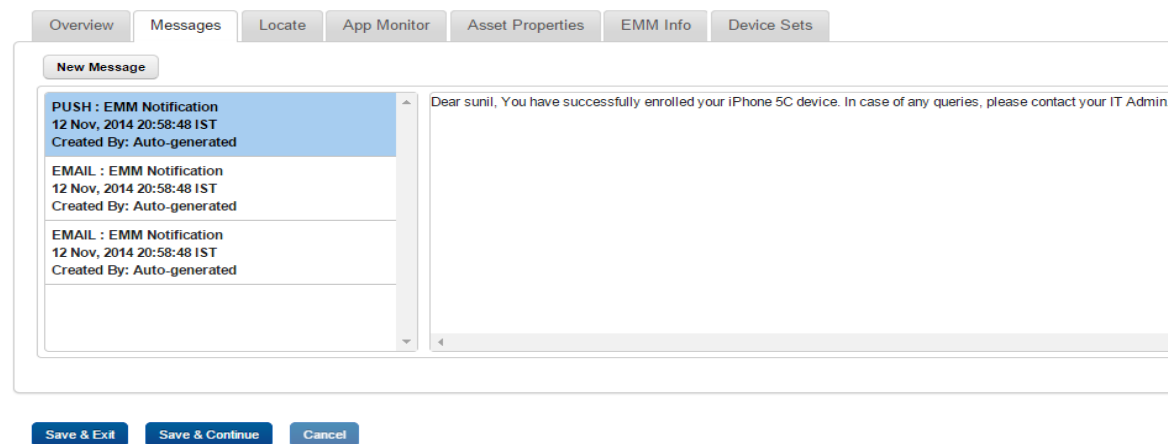


The message appears in the message window

7. **Personalization Attributes:** Select the required attribute from the dropdown list. These details are populated through Active Directory.

The Personalized Attributes are predefined and system displays the related details as per the selected attributes. For example, if you select Device OS, Device Name, and the Device Model No from the dropdown list. The respective details are picked up from the device and appended in the sent message.

8. Click the **Add** button. The details appear in the Message Box.
9. Click the **Send** button to submit the message. In the confirmation message (Send Message - Success) that appears, click **OK** to continue.



The message appears in the message window.

Locate

The Locate Tab displays the location details. You may wish to know the location of a device under several situations. For example,

- The device is out of compliance and you wish to take some action against the same.
- You receive an alert on the device.
- User is traveling.
- User is absent without notice for a while.

Last Known Location

A.  H-08
 03:27 IST
 17.447296 78.371079
 H-08, Rolling Hills, Gachibowli, Hyderabad,
 Andhra Pradesh 500081, India

Last Five Locations [map all](#)

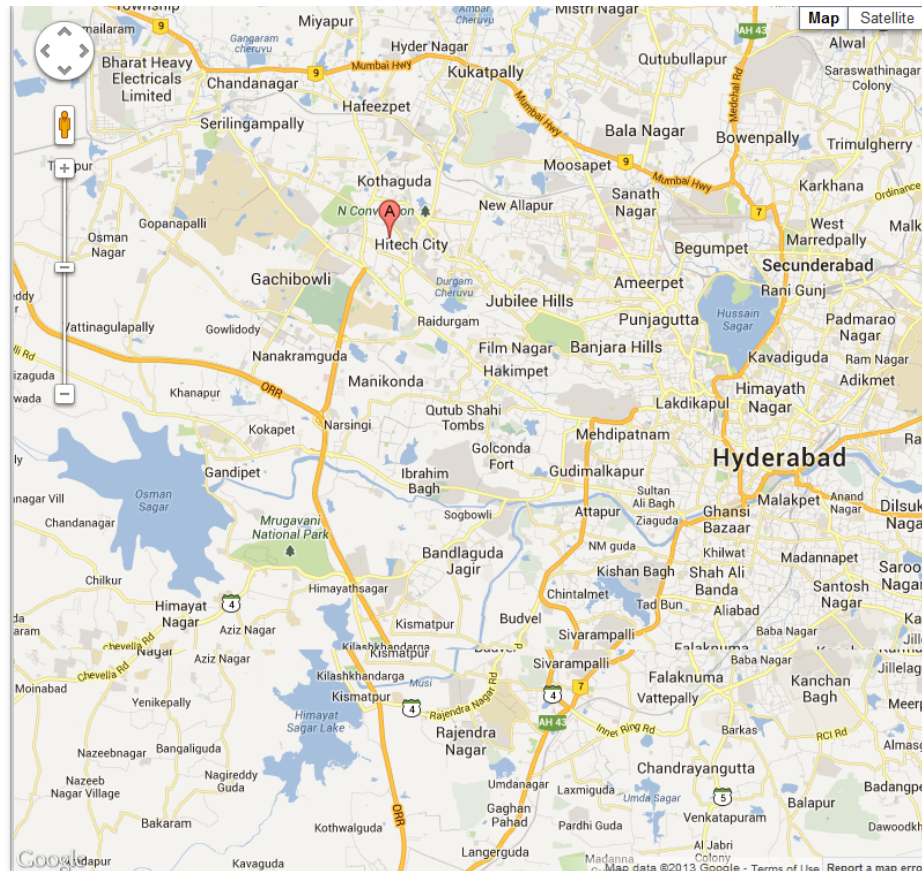
B. H-08, Rolling Hills, Gachibowli, Hyderabad,
 Andhra Pradesh 500081, India
 03:27 IST
 17.447393 78.371048

C. H-08, Rolling Hills, Gachibowli, Hyderabad,
 Andhra Pradesh 500081, India
 03:20 IST
 17.447296 78.371080

D. H-08, Rolling Hills, Gachibowli, Hyderabad,
 Andhra Pradesh 500081, India
 03:08 IST
 17.44713370689884 78.37106321014312

E. H-08, Rolling Hills, Gachibowli, Hyderabad,
 Andhra Pradesh 500081, India
 10:00 IST

F. H-08, Rolling Hills, Gachibowli, Hyderabad,
 Andhra Pradesh 500081, India
 09:56 IST
 17.44713370689884 78.37106321014312



You can view the most recently polled location of the device both in terms of coordinates as well as the address as indicated by the used maps service.

You can also view the last 5 locations of the device as per the location samples collected. The system displays the following location information about the device:

- Current location
 - Location Address (as provided by the maps software used)
 - Time of Polling (Time specified in UTC)
 - Map (with pinned location) with latitude and longitude details

- Past 5 locations
 - Location Pin Name
 - Location Addresses
 - Time of Polling

You can zoom in and zoom out as required.

Important: If location is turned off on device, then portal does not display the map with last five locations.

Note: If you are using a free Google Maps license, when the limit is reached you will see an error - 'Geo coder failed due to:OVER_QUERY_LIMIT'. In such cases it is recommended to move to a business license.

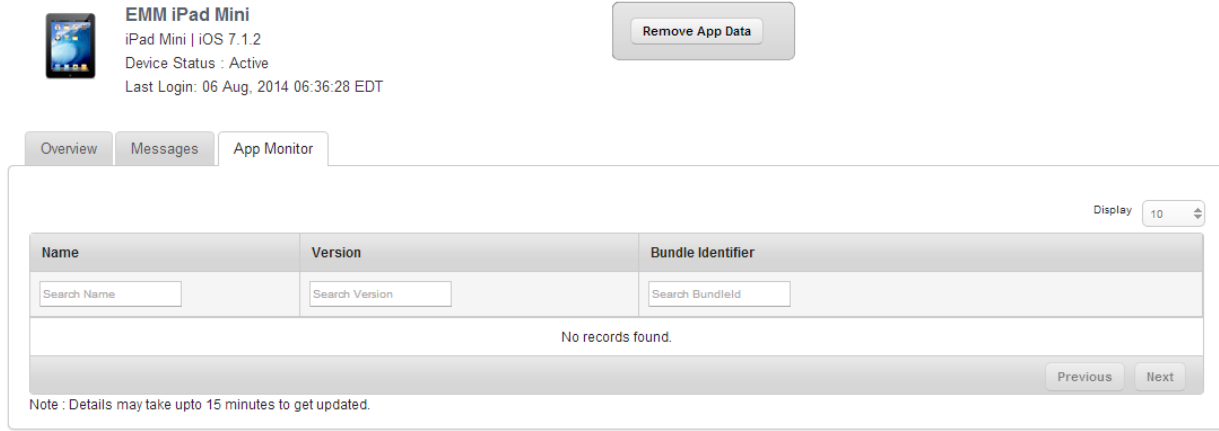
App Monitor

The App Monitor displays the installed apps on a device. It does not display default apps that are installed with OS.

- **Installed Apps:** Installed Apps section displays all apps that are installed on the device. Details of installed apps and app details vary based on the operating system of the device. You can find more details on it in the sections below specific for each OS.
- **Targeted Apps:** This section displays all apps targeted to a device but not installed on the device.

There are types of Apps shown.

App Monitor for iOS



EMM iPad Mini
iPad Mini | iOS 7.1.2
Device Status : Active
Last Login: 06 Aug, 2014 06:36:28 EDT

Remove App Data

Overview Messages App Monitor

Display 10

| Name | Version | Bundle Identifier |
|--|---|---|
| <input type="text" value="Search Name"/> | <input type="text" value="Search Version"/> | <input type="text" value="Search Bundlefield"/> |
| No records found. | | |

Previous Next

Note : Details may take upto 15 minutes to get updated.

The App Monitor list view for iOS has the following details:

- **Name:** Displays the Name of the application.
- **Version:** Displays the Version of the application.
- **Bundle Identifier:** Displays the bundle ID of the application.

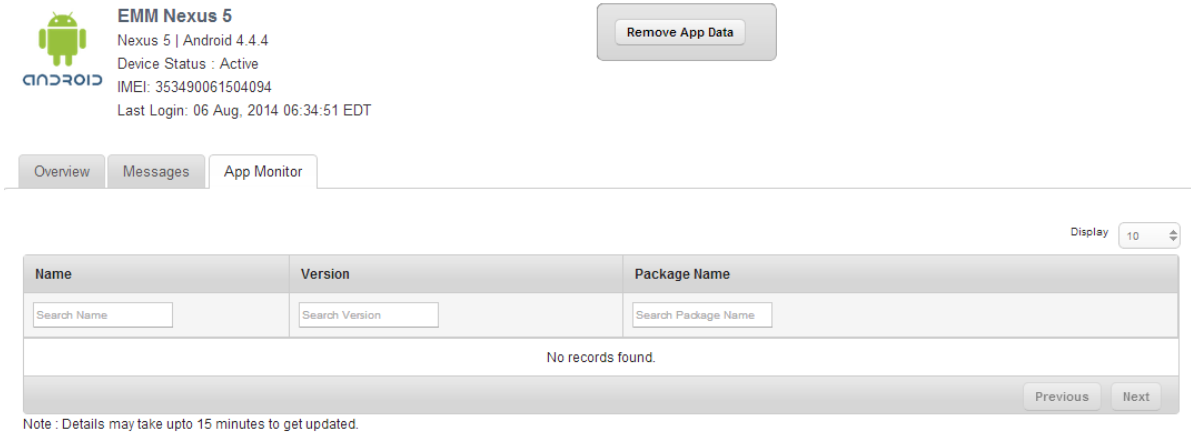
Note: In the App Monitor tab for iOS, Publisher has been replaced with Bundle Identifier.

App Monitor for Android

You can search a desired app through search filters based on all grid columns. You can apply a single or a combination of search filters to define the search criteria and get the refined outcome.

Device Details

[Device List](#) > Device Details



EMM Nexus 5
 Nexus 5 | Android 4.4.4
 Device Status : Active
 IMEI: 353490061504094
 Last Login: 06 Aug, 2014 06:34:51 EDT

[Remove App Data](#)

Overview Messages **App Monitor**

Display 10

| Name | Version | Package Name |
|--|---|--|
| <input type="text" value="Search Name"/> | <input type="text" value="Search Version"/> | <input type="text" value="Search Package Name"/> |
| No records found. | | |
| | | Previous Next |

Note : Details may take upto 15 minutes to get updated.

The App Monitor list view for Android SAFE devices has the following details:

To search for an app, follow these steps:

1. **Name:** Displays the Name of the application.
2. **Version:** Displays the Name of the application.
3. **Package Name:** Displays the package name of the application.

9.3.3.2 Device Details Page Actions

You can perform the following activities from Device List page.

- [Searching for Devices](#)
- [Updating Device Details](#)
- [Locking a Device](#)
- [Remove App Data](#)

Searching for Devices

You search for devices through search filters based on all grid columns. You can apply a single or a combination of search filters to define the search criteria and get the refined outcome. To search a device, follow these steps:

| | Device Name ▼ | Device Owner | OS | Last Login | Date of First Login | Status |
|--------------------------|---|--|--|-------------------------------|-------------------------------|---|
| | <input type="text" value="Search Device Name"/> | <input type="text" value="Search Device Owr"/> | <input type="text" value="Search OS"/> | All ▾ | All ▾ | |
| <input type="checkbox"/> | EMM iPad Mini | EMM Admin | 🍏 iOS 7.1.2 | 06 Aug, 2014 06:36:28 E DT | 06 Aug, 2014 06:36:28 E DT | <input type="button" value="Deactivate"/> |
| <input type="checkbox"/> | EMM Nexus 5 | EMM Admin | 🤖 Android 4.4.4 | 06 Aug, 2014 06:34:51 E DT | 06 Aug, 2014 06:34:51 E DT | <input type="button" value="Deactivate"/> |


1. Enter or select details for the following search filters:
 - a. **Device Name:** Enter partial or a complete device name in the **Search Device Name** text field.
 - b. **Status:** Select the desired option from the drop-down list.
 - c. **Device Owner:** Enter partial or a complete owner name in the **Search Device Owner** text field.
 - d. **Ownership:** Select the required category from the dropdown list.
 - e. **OS:** Enter desired operating system version in the **Search OS** text field.
 - f. **Last Log in:** Shows several options to shortlist the Last Log in by.
 - g. **Date of First Login:** This is the date of registration of the device.
2. According to your search filter criteria, the list view is updated with respective device details. By default, the list view displays ten devices according to Display settings, which you can modify through Display dropdown list. You can also scroll the list view through **Previous** and the **Next** buttons.

Remove App Data

Remove App Data is only applicable to Enterprise Apps that are wrapped-signed and pushed through EMM and not for side-loaded apps. This action is performed to remove all the data from the apps. This action is performed by an enterprise store to retain the apps but remove the app data to retain safety.

Device Details

[Device List](#) > Device Details



EMM iPad Mini
iPad Mini | iOS 7.1.2
Device Status : Active
Last Login: 06 Aug, 2014 06:36:28 EDT

[Remove App Data](#)

Overview Messages App Monitor

To remove the data from the apps, follow these steps:

1. Click the required device in the list view.

The **Device Details** page appears.

2. Click the **Remove App data** button.

The System displays the warning message (**Remove App Data**) asking the user, if really wishes to remove all the corporate data from the device.

3. Click the **Remove** button to remove the app data. In the confirmation message (Remove App Data) that appears, click **OK** to return to the page.

Note: For Windows Phone 8.x devices, the remove app data policy will not work if the app is in use. The policy command will apply when the app is closed and relaunched.

Note: If this is applied for non-supervised devices, the command will not execute.

10. App Management

Kony EMM allows the administrator to control the app usage of device users in several ways. Kony provides an App Store where all the Enterprise Apps required by employees of the company are stored. Administrators can add apps to this store, attach them to categories and also distribute them from here to targeted individual device users.

App Management also allows the administrator to inject policies into these apps so that their usage can be controlled as per the IT policies of the company.

App Management also allows the creation of Categories to which apps can be assigned. This helps users to find requisite apps more easily.

App Management currently supports the following platforms:

Important: Browser apps are not supported as Enterprise apps.

- iOS phone devices
- iPads
- Android phones
- Android tablets
- Windows Phone 8.x

Note: For Windows Phone 8.x apps, only C# XAML based apps are supported for wrapping and signing.

No other platforms are currently supported.

10.1 App Classification

Apps which are downloaded directly through public app stores such as Apple App Store or Google Play are referred as Public Apps. These include apps such as Facebook, Twitter, Evernote and so on.

Apps that are uploaded by the Admin into the Enterprise Store and distributed from there to devices are Enterprise Apps. These would include apps built by the company or custom built for the company to be distributed among employees. It can also include apps, which are specifically licensed to be distributed. For example: Consumer Goods companies provide a mobile based sales tracking application to their sales people. This is a classic enterprise app as it is built by the company for internal usage.

Some apps available on Public App Stores are again specifically made available through the Enterprise Store. In this scenario, these apps are also considered as Enterprise Apps.

App Management module allows you to store and manage all versions of the apps that you wish to install, update or remove from the devices.

10.2 Managing Apps

Managing applications includes:

- [Policies](#)
- [Categories](#)
- [Enterprise Apps List](#)

10.3 Policies

When you add an Application on devices, you need to specify an application control policy. Policies control the data that Applications can access on devices. You can create custom policies or change the default settings of the standard application control policies.

From the **App Management** section, click **Policies** from the left panel. The **Policies** page appears with a list of the policies. The list view displays a list of all the policies along with their State and Statuses. You can search the policies based on each column and also sort on each column.

| <input type="checkbox"/> | Policy Name | Last Modified On | State | Owner | Status |
|--------------------------|--|----------------------------------|---|---|---|
| | <input type="text" value="Search Policies"/> | <input type="text" value="All"/> | <input type="text" value="All States"/> | <input type="text" value="Search Owner"/> | <input type="text" value="All Statuses"/> |
| <input type="checkbox"/> | iOS Policy | 03 Jul, 2015 05:47:07 EDT | Active | admin | Published |
| <input type="checkbox"/> | EMM Policy | 03 Jul, 2015 05:46:41 EDT | Draft | admin | Unpublished |

Page (1/1)

The Policies list view displays the following columns:

| Columns | Description |
|------------------|--|
| Policy Name | Displays the unique identification name of the policy. |
| Last Modified On | Displays the date on which the policy was last updated. |
| State | Displays the current state of the policy for example, Active or Draft. |
| Owner | Displays the administrator user name. |
| Status | Displays the current status of the policy for example, Published or Unpublished. |

You can perform following activities from this page:

- [Creating a New Policy](#)
- [Applying Policies](#)

- [Searching for Policies](#)
- [Updating a Policy](#)
- [Deleting a Policy](#)

10.3.1 Creating a New Policy

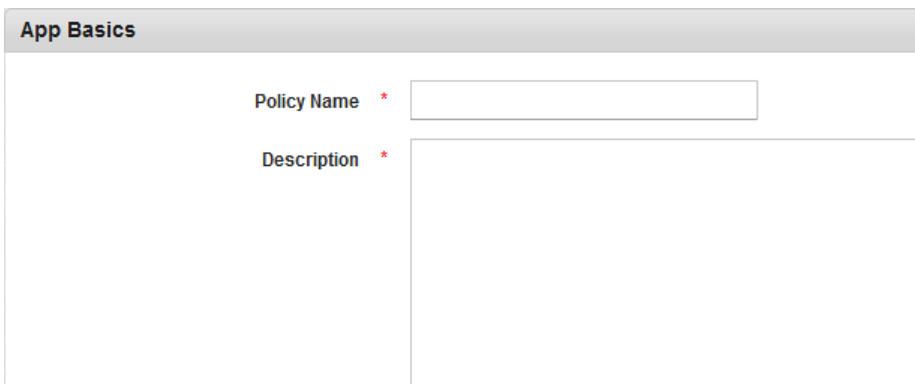
When a new app is registered, the administrator must decide if it should be protected by a policy. Click **+New Policy** button on Policies main screen to open **New Policy** screen.

The New Policy screen includes following sections:

- [App Basics](#)
- [App Usage](#)
- [Network](#)
- [Storage](#)
- [Phone Features](#)

10.3.1.1 App Basics

The app basics section refers to adding a title and description to the new policy. To add app basics, follow these steps:



App Basics

Policy Name *

Description *

1. **Policy Name:** Enter a unique name for the new app policy. The policy name should not include \ / : * ? " < > | , special characters. If the entered policy name already exists, the system displays the error message.
2. **Description:** Enter a description for the new app policy. The description should accurately describe the features and functionality of your policy.

10.3.1.2 App Usage

The App Usage section allows you to configure an app usage policy. To add details, follow these steps:

App Usage

App Lockout Yes No

Geofence Rule Allow Restrict

Time Fence Rule Allow Restrict

Idle Timeout minutes Expire Launchpad Session Android

Expiration Date

Note Leave blank to never expire

Allow Copy, Cut, Paste Yes No

Allow Camera Access Yes No

Allow Document Sharing Yes No

Allow Screen Capture Yes No Android

Device Policy

1. **App Lockout:** Based on your requirement, select the option as Yes or No. If App Lockout is set to Yes, the app shall be locked out for the targeted users. If App Lockout is set to No, the users shall be able to launch the app. This is the default choice. The feature enables the admin to ensure that the app cannot be launched anymore, irrespective of the expiry time limit. This is typically used as a temporary measure or as a means of creating an exception for a user who belongs to a targeted Group and so on.

2. **Geofence Rule:** By default, this option is set to **Allow**. You can change it to **Restrict**.

- a. Select the required Geofence rule from the drop-down list. The Add button appears. Click the **Add** button to add the Geofence rule. The selected Geofence rule appears in a list view.

| Geo Fence Name | |
|----------------|-------------------------|
| konyfence | <button>Remove</button> |

- b. Click the **Remove** button to remove the selected Geofence rule.

Geofence programs enable an administrator to set up triggers so when a device crosses a geofence and enters or exits the borders demarcated by the administrator, an SMS or an email alert is sent. For example, geofence enables a mobile device to setup the places that matter most to you and interact at those locations. Once a user enters into your geofence configuration, you can communicate based on defined policies.

Note: When the device is offline, User can access the app by mocking device's GPS location.

3. **Time Fence Rule:** Select the required Time Fence rule from the drop-down list. By default, it is set to **Allow**. You can change it to **Restrict**.

Time fences enable you to establish policies for prioritizing activities. Time fences are points in time where you can define how a defined policy rule is applied to an app deployed on a device.

When a time fence policy is pushed to registered device, the policy will be fetched based on server time and time zone configured in Device Settings page. Policy reflection is not dependent on device time and time zone as long as the device is online.

Note: If the device is offline mode, user can access the app by changing the device time.

When the device is offline, the device cannot communicate with the EMM server and therefore must rely on device time to implement time related rules. Therefore there is a possibility for the User to manipulate device time to bypass some of the rules.

4. **Idle Timeout:** Set the idle timeout for the device in minutes.

Idle Time out means that, if the application does not use the connection to the device for scheduled time period, then connection is closed automatically.

5. **Expire Enterprise Store Session:** Select this if you want the enterprise store session to expire after the Idle timeout time. This feature is applicable only for Android devices.
6. **Expiration Date:** This is the date on which app policy is no longer valid or in effect. To set the expiration date for the app policy, Click in the text field to open the Calendar window.

The image shows a mobile interface for setting an expiration date and time. At the top, a calendar for February 2014 is displayed with the 25th highlighted. Below the calendar, the current time is shown as 17:22. There are two sliders: one for the Hour (set to 17) and one for the Minute (set to 22). At the bottom of the time picker are three buttons: 'Minimum', 'Clear', and 'Done'.

Expiration Date

Select the date. Select the required Time - Zone through the slider. Click **Done** to continue. The date and time appears in the text field.

Expiration Date Leave blank to never expire

When an app expiry policy is pushed to registered device, the policy will be fetched based on server time and time zone selected in Device Settings page. Policy reflection is not dependent on device time and time zone as long as the device is online.

Note: If the device is offline mode, user can access the app by changing the device time.

When the device is offline, the device cannot communicate with the EMM server and therefore must rely on device time to implement time related rules. Therefore there is a possibility for the User to manipulate device time to bypass some of the rules.

7. **Allow Copy, Cut, Paste:** Select the **Yes** option to allow the Cut, Copy, and Paste options within the app. Select the No option to not allow Cut, Copy, and Paste options.
8. **Allow App Camera Access:** Select **Yes** to enable App Camera to capture movies and still images. Select the No option to deny the access.
9. **Allow Document Sharing:** Select **Yes** to enable sharing of documents with multiple people. Select the No option to deny the access.
10. **Allow Screen Capture:** Configure to **Yes** to enable screen capturing on the app. This is applicable only for Android devices.
11. **Device Policy:** Select the device restriction policy from the available policy list.

10.3.1.3 Network

This section enables an administrator to define the policy to support network access at the functional level. The declared policy set is enforced by the app. To configure the network, follow these steps:

Network

Allow Offline Access Yes No

Allow Network Access Yes No

Force HTTPS Yes No

Domains Restriction Allow all except below Restrict all except below

*

You have 1999 characters left

Wifi SSID Access Allow all except below Restrict all except below

*

You have 1999 characters left

1. **Allow Offline Access:** By default this option is set to **No**.

You can modify it to **Yes** to give device users access to Enterprise Apps installed from their devices when the devices are offline.

Enterprise apps installed on devices can be accessed online or offline based on the policy assigned to the app and target. When a device is offline, a user can only launch apps through enterprise store - My Apps.

2. **Allow Network Access:** Select the **Yes** option to Allow Network Access or the **No** option to restrict the Network Access.
3. **Force HTTPS:** Select the **Yes** option to enable **Force HTTPS**. Select the **No** option to disable Force HTTPS.

Force HTTPS option forces every user request to access the device via HTTPS.

4. **Domains Restriction:** By default Domain Restriction, option is set to **Allow all except below**. You can modify it to **Restrict all except below**. Enter the domains you wish to restrict into the text box.
5. **WiFi SSID Access:** By default WiFi SSID Access is set to **Allow all except below**. You can change it to **Restrict all except below**. Enter the SSID details you wish to restrict into the text box.

10.3.1.4 Storage

The Storage section enables you to configure secure data storage on your device. To configure data storage, follow these steps:

Storage

Allow External Storage Read Yes No
Note Supported only for Android and Windows devices.

Allow External Storage Write Yes No
Note Supported only for Android and .appx apps on Windows devices.

Encrypt App SQLite Data Storage Yes No
Note Encrypt App SQLite Data Storage is not applicable to Windows devices

1. **Allow External Storage Read:** By default, this is set to **Yes**. This is supported only for Android and Windows devices.
2. **Allow External Storage Write:** By default, this is set to **Yes**. This is supported only for Android and .appx apps on Windows devices.
3. **Encrypt App Data Storage:** Select the Yes option to enable data encryption and select the No option to deny it. Encrypt App SQLite Data Storage is not applicable to Windows devices.

Encrypted Data Storage lets you store your files in the encrypted container to check any unauthorized access to vital information.

Important: As part of wrapping, SQLite is replaced with SQLCipher. SQLCipher is used for database encryption. There is a subtle difference between SQLCipher and SQLite. In your app, if string data (i.e. base64 string for image) is stored in blob column then it works for SQLite and not SQLCipher. Please ensure that string data is stored in column with 'TEXT' data type and binary data is stored in column with 'BLOB' data type.

Important: Kony Management provides SQLCipher where native libraries (.so files) are built with ARM 32-bit and X86 architectures. Kony Management does not provide SQLCipher libraries built for 64-bit ARM architectures. A child app which contains 64-bit arm libraries will not work after wrapped with Kony Management. The child app should not contain any 64-bit arm libraries for it work properly in Kony Management environment.

Important: Kony Management uses SQLCipher version 3.5.7. If you use a higher version of SQLCipher than 3.5.7 and build your app, while wrapping, Kony Management will downgrade the SQLCipher version to 3.5.7.

10.3.1.5 Phone Features

This is to allow this particular feature to be used by the App or not. The list is to whom an SMS, Email or Phone can be made. To set the phone features, follow these steps:

Phone Features

SMS App Usage Allow all except below Restrict all expect below

Comma separated phone numbers

Email Usage Allow all except below Restrict all expect below

Comma separated email addresses

Phone Usage Allow all except below Restrict all expect below

Comma separated phone numbers

1. **SMS App Usage:** By default SMS App Usage option is set to **Restrict All Except Below**. You can modify it to **Allow All Except Below**. Enter the phone numbers that you wish to restrict or allow.
2. **Email Usage:** By default Email Usage option is set to **Restrict All Except Below**. You can modify it to **Allow All Except Below**. Enter the email IDs that you wish to restrict or allow.
3. **Phone Usage:** By default Phone Usage option is set to **Restrict All Except Below**. You can modify to **Allow All Except Below**. Enter the phone numbers that you wish to restrict or allow.
4. Click the **Save and Submit** button to save the details. The new policy appears in the list view
5. Click the **Save and Continue** button to Save the details and stay on the same page to update other details.

Click the **Cancel** button to close the window.

10.3.1.6 Supported actions for Webview in App Policy

For apps where app policy restrictions are applied, if the apps allow webview within the app, then not all app policy restrictions are applicable for the webview. See the image below for applicable restrictions.

Supported actions for Webview App Policy

| Action | Windows phone 8.x (XAP) | Windows phone 8.x (APPX) | Android | IOS |
|---------------------------------|-------------------------|--------------------------|---------|-----|
| Copy-Paste | ✗ | ✗ | ✓ | ✓ |
| Document sharing | ✗ | ✗ | ✓ | ✓ |
| Network | ✓ | ✓ | ✓ | ✓ |
| Phone Features | ✓ | ✗ | ✓ | ✓ |
| Encrypt App SQLite Data Storage | ✓ | ✗ | ✓ | ✓ |
| External Storage Read | ✓ | ✓ | ✓ | ✗ |
| External Storage Write | ✗ | ✓ | ✓ | ✗ |

10.3.2 Applying Policies

Policies are applied when they are targeted to Users. [Targeting](#) can happen while creating an app, editing an app, upgrading an app, or adding a new platform.

Policies are applied for an app to a particular target (User/Group) that makes them very personalized. When policies are applied to Groups, a priority must also be assigned. Policies assigned to Users have the highest priority.

10.3.3 Searching for Policies

You can search a policy through search filters based on all grid columns. You can apply a single or a combination of search filters to define the search criteria and get the refined outcome.

| <input type="checkbox"/> | Policy Name | Submitted | State | Owner | Status |
|--------------------------|--|------------------------------------|---|---|---|
| | <input type="text" value="Search Policies"/> | <input type="text" value="All"/> ▾ | <input type="text" value="All States"/> ▾ | <input type="text" value="Steven Smith"/> | <input type="text" value="All Statuses"/> ▾ |

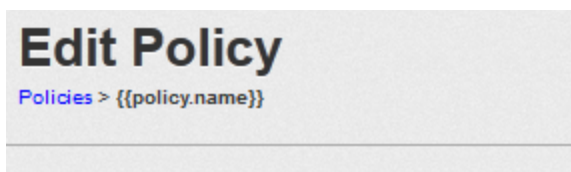
1. To search a policy, follow these steps:
 - a. **Policy Name:** Enter partial or a complete policy name in the **Search Policies** text field.
 - b. **Submitted:** Enter the date on which the device policy was submitted in the **Submitted Date** text field.
 - c. **State:** Select the desired option from the drop-down list, for example, Active or Draft.
 - d. **Owner:** Enter partial or the complete name of the administrator in the text field.
 - e. **Status:** Select the desired option as All Statuses, Unpublished or Published.
2. According to your search filters criteria, the list view is updated with respective policy details. By default, the list view displays ten policies according to Display settings, which you can modify through Display dropdown list. You can also scroll the list view through Previous and the Next buttons.

10.3.4 Updating a Policy

You may need to update a policy detail for specific reasons, for example, you may need to update a policy name or its description.

| <input type="checkbox"/> | Policy Name | Click Policy Name to edit the policy |
|--------------------------|---------------|--------------------------------------|
| <input type="checkbox"/> | Sample Policy | |

Click the Policy Name. **Edit Policy** page appears.



All the fields in the policy can be updated. There are no restrictions. Once a policy is updated, it must be published again to come into effect, else the older policy continues to be effective.

Note: When EMM 2.0 is upgraded to EMM 2.1, all App Policies might require administrators to take ownership of the same (even those created by the same admin)

10.3.5 Deleting a Policy

If a policy has been deprecated, or no longer required, you can delete it.

| <input type="checkbox"/> | Policy Name | Last Modified On | State | Owner | Status |
|-------------------------------------|--|----------------------------------|---|---|---|
| | <input type="text" value="Search Policies"/> | <input type="text" value="All"/> | <input type="text" value="All States"/> | <input type="text" value="Search Owner"/> | <input type="text" value="All Statuses"/> |
| <input type="checkbox"/> | iOS Policy | 03 Jul, 2015 05:47:07 EDT | Active | admin | Published |
| <input checked="" type="checkbox"/> | EMM Policy | 03 Jul, 2015 05:46:41 EDT | Draft | admin | Unpublished |

Page {1/1}

1. Select the policy through check box next to it in the list view. This action activates the **Delete** button.
2. Click the **Delete** button. In the warning message (Delete Policy(s) that appears, click **Yes** to continue.
3. In the success message that appears, click **OK** to continue.

The policy is no longer displayed in the list view. Only unpublished policies can be deleted.

10.4 Categories

From the **Categories** section, you add all the categories. Categories are not pre-defined. All the Categories must be added through this section and then only can be assigned to apps.

For example, financial applications can have a category named as Money Manager, which facilitates record keeping for the bank accounts, transactions entry and view the balance details. The other categories can be Banking Payment, ATM Finders, Insurance, and Taxes Portfolio and so on. You can update or delete or assign apps to these categories.

From the **App Management** section, click **Categories** from the left panel. The Categories page appears with a list of the Categories. You can search the categories based on each column and also sort on each column.

The screenshot shows the 'Categories' management interface. At the top left is the title 'Categories' and a '+ New Category' button. Below this is a table with two columns: 'Category Name' and 'Created By'. The table contains one entry: 'General' under 'Category Name' and 'admin' under 'Created By'. There are search input fields for both columns. At the bottom of the table, there are buttons for 'Delete', 'Previous', 'Page {1/1}', and 'Next'. A pagination indicator at the top right shows 'Displaying 1 - 1 of 1 - Display 10'.

The Categories list view displays the following columns:

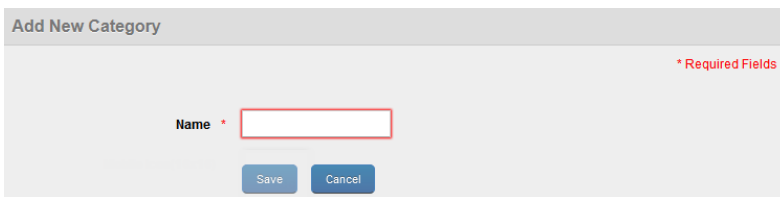
| Columns | Description |
|------------|--|
| Name | Provides a list of all the categories. |
| Created By | Provides a list of all the administrators. |

You can perform following activities from this page:

- [Creating a New Category](#)
- [Searching for Categories](#)
- [Updating a Category](#)
- [Deleting a Category](#)

10.4.1 Creating a New Category

Click the **+New Category** button on **Categories** main screen to open **Add New Category** window. To create a new Category, follow these steps:



1. **Category Name:** Enter a unique name for the category.
2. Click the **Save** button. In the success message that appears, click OK to continue. The newly added category appears in the list view.

Click the **Cancel** button to close the window.

Field with the red asterisk sign is mandatory.

10.4.2 Searching for Categories

You can search a desired category through search filters available. You can apply a single or a combination of search filters to define the search criteria and get the refined outcome.

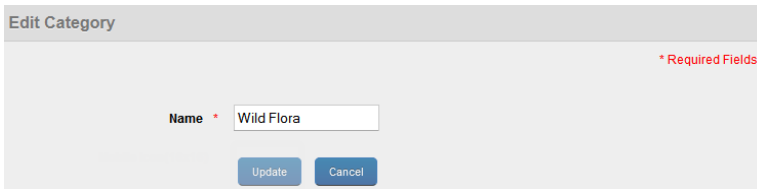


1. To search a category, follow these steps:
 - a. **Name:** Enter partial or a complete category name in the **Category Name** text field
 - b. **Created By:** Enter partial or the complete name of the administrator in the text field..
2. According to your search filters criteria, the list view is updated with respective category details. By default, the list view displays ten categories according to Display settings, which you can modify through Display dropdown list. You can also scroll the list view through Previous and the Next buttons.

10.4.3 Updating a Category

The primary purpose to a update a Category details is to fulfill the requirement of existing business rules.

To update details for the required fields, follow these steps:

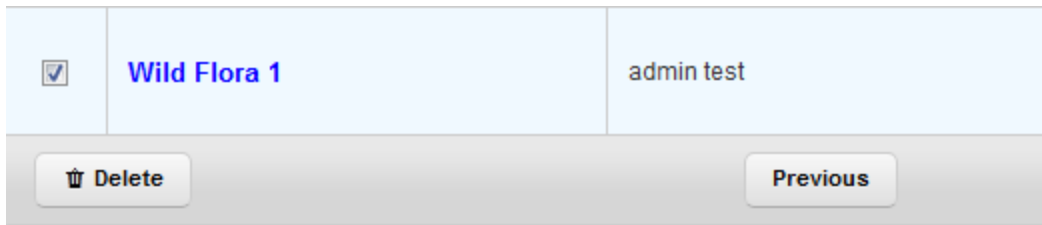


1. **Category Name:** If required, change the category name.
2. After all the updates, the Update button becomes active.
3. Click the **Update** button. In the confirmation message that appears, click OK to continue.

Click the **Cancel** button to close the window.

10.4.4 Deleting a Category

If a category has been deprecated, or no longer required, you can delete it.



To delete a category, follow these steps:

1. Select the category through check box next to it in the list view. This action activates the **Delete** button.
2. Click the **Delete** button. In the warning message that appears, click **Yes** to confirm the deletion of the category.
3. In the success message that appears, click OK to continue.

The category is no longer displayed in the list view.

10.5 Enterprise Stores

An enterprise store allows you to define and use a branding set for your users and groups. You can define the required branding based on your specific requirements.

Important: Ensure that you upgrade to Enterprise Store of V8 GA release before upgrading your iOS device to iOS 11. If you upgrade to iOS 11 before upgrading the enterprise store, kill the enterprise store and download it again using your enterprise store download URL.

An administrator can assign any of the branding set to any user or group in Kony Management server.

The Enterprise Store helps you to create a clone of an existing Enterprise Store app, apply a separate branding set, and then target it to a specific set of users/groups.

From the **App Management** section, click **Enterprise Stores** from the left panel. The Enterprise Stores page appears. This page displays a list of enterprise stores along with their versions and other information such as branding set, targets, and priority.

Enterprise Stores

[+ New Enterprise Store](#)

Note: Branding, Targeting and Re-Prioritization not available for Enterprise Stores currently being signed

| Priority | Name | Branding Set | Targets |
|------------------|------------|--------------|----------------------|
| 1 | Launchpad2 | Premtest | Edit |
| Lowest (Default) | Launchpad | DEFAULT | None (Default) |

[Change Enterprise Store Priorities](#)

The Enterprise Stores view displays the following columns:

| Columns | Description |
|------------------------------------|--|
| Priority | Displays the enterprise store priority. |
| Name | The unique name of a store as specified by you while creating the enterprise store. It is unique. |
| Branding Set | You can assign a branding set for an enterprise store. The set appears in the column. You can change the branding set if required from the list. You can get more information about branding sets from the Branding page . |
| Targets | By default, the column is configured to None (Default) . You can edit the targets. |
| Change Enterprise Store Priorities | You can change the priority order of an enterprise store using the button. The feature is used when a user is assigned more than one enterprise store through multiple group targeting. |

You can perform the following activities from the **Enterprise Stores** page:

- [Creating a New Enterprise Store](#)
- [Modifying a Branding Set for an Enterprise Store](#)

- [Editing Targets for an Enterprise Store](#)
- [Changing Enterprise Store Priorities](#)

10.5.1 Creating a New Enterprise Store

For Android devices, the Enterprise store binary will be named based on the enterprise store name you provide. For example, if your enterprise store name is **Company App**, the .apk will be named as **CompanyApp.apk** for Android phones and **CompanyApptablet.apk** for Android tablets.

Important: Ensure that the Enterprise store name you provide (in the Branding section) does not contain # sign in it. If the Enterprise store name has a # sign in it, downloading the enterprise store on the Samsung native browser will fail.

To create a new enterprise store, follow these steps:

1. In Kony Management Suite Management console, click **Enterprise Stores**. The Enterprise Stores page appears.
2. Click **Add New Enterprise Store**. The Create New Enterprise Store page appears.
3. In the **Name** field, enter the enterprise store name.
4. From the **Branding** list, select the branding set you want to apply on the enterprise store. The **Create** button is enabled.
5. Click **Create**. The **Confirm Action** page appears.

Note: You cannot delete an enterprise store once it is created.

6. Click **Yes**. A **Success** page appears.

7. Click **OK**. The new enterprise store is created and appears in the Enterprise Stores page.

Important: The enterprise store status can be "Signing in progress" for some time. The new enterprise store will also appear in the **Enterprise Apps** page.

10.5.2 Modifying a Branding Set for an Enterprise Store

To modify the branding set for an enterprise store, follow these steps:

1. In Kony Management Suite Management console, click **Enterprise Stores**. The Enterprise Stores page appears.
2. From the Branding Set list, select the branding set you want to apply to the enterprise store. The **Confirm Action** page appears.
3. Click **Yes**. A **Success** page appears.
4. Click **OK**. The branding set for the enterprise store is modified.

10.5.3 Editing Targets for an Enterprise Store

To edit targets for an enterprise store, follow these steps:

1. In Kony Management Suite Management console, click **Enterprise Stores**. The Enterprise Stores page appears.
2. In the Targets column, click **Edit** for the enterprise store where you want to modify targets. The **Targeting** page appears.
3. In the **Users** tab, select the users you want to target.
4. Click the **Groups** tab. The Group details appear.
5. Select the groups you want to target.
6. Click **Save**. The Confirm Action page appears.

7. Click **Yes**. The Success page appears.
8. Click **OK**. The page closes and the targets are modified.

10.5.4 Changing Enterprise Store Priorities

To change priorities for an enterprise store, follow these steps:

1. In Kony Management Suite Management console, click **Enterprise Stores**. The Enterprise Stores page appears.

Enterprise Stores

+ New Enterprise Store

Note: Branding, Targeting and Re-Prioritization not available for Enterprise Stores currently being signed.




| Priority | Name | Branding Set | Targets |
|------------------|------------|--------------|----------------|
| 1 | Launchpad2 | DEFAULT | Edit |
| 2 | Premtest | Premtest | Edit |
| 3 | Testdocs | DEFAULT | Edit |
| Lowest (Default) | Launchpad | DEFAULT | None (Default) |

Change Enterprise Store Priorities

2. Click **Change Enterprise Store Priorities**. The Priority column is editable.

Enterprise Stores

Note: Drag the unlocked Enterprise Store entries to change priority. Changes will not take effect till you save.

| Priority | Name | Branding Set | Targets |
|---|------------|--------------|-------------------------------------|
| 1 →  | Launchpad2 | DEFAULT | <input type="button" value="Edit"/> |
| 2 →  | Premtest | Premtest | <input type="button" value="Edit"/> |
| 3 →  | Testdocs | DEFAULT | <input type="button" value="Edit"/> |
| Lowest (Default) | Launchpad | DEFAULT | None (Default) |

3. Drag and move the enterprise store in the priority column based on your requirements.

Enterprise Stores

Note: Drag the unlocked Enterprise Store entries to change priority. Changes will not take effect till you save.

| Priority | Name | Branding Set | Targets |
|------------------|------------|--------------|-------------------------------------|
| 3 → ① | Testdocs | DEFAULT | <input type="button" value="Edit"/> |
| 1 → ② | Launchpad2 | DEFAULT | <input type="button" value="Edit"/> |
| 2 → ③ | Premtest | Premtest | <input type="button" value="Edit"/> |
| Lowest (Default) | Launchpad | DEFAULT | None (Default) |

4. Click **Save Priority Changes**. The Confirm Action page appears.
5. Click **Yes**. The Success page appears.
6. Click **OK**. The Priority order of the enterprise stores is modified.

10.6 Enterprise Apps

Enterprise apps are typically designed to be used within the organization while meeting strict requirements for security and administration management. Enterprise apps are used to manage several tasks. For example, Business-to-employee (B2E) productivity mobile applications automate employee-related corporate processes, such as, Expense Management and Online Supply Request.

From the **App Management** section, click **Enterprise App List** from the left panel. The Enterprise Apps List page appears. This page displays a list of apps along with their versions and other information such as Wrap Condition, Workflow, State, Current Owner and Publish Status. You can search the apps based on each column and also sort on each column.

Enterprise Apps

[+ New Enterprise App](#)

Displaying 1 - 10 of 12 - Display

| <input type="checkbox"/> | App Name | Platform | Version | Licenses | Wrap Condition | Workflow State | Current Owner | Publish Status |
|--------------------------|--|--|---------|-----------|----------------------------------|---|---|---|
| | <input type="text" value="Search Apps"/> | <input type="text" value="All Platforms"/> | | | <input type="text" value="All"/> | <input type="text" value="All States"/> | <input type="text" value="Search Owner"/> | <input type="text" value="All Statuses"/> |
| <input type="checkbox"/> | contoso Category: General | Windows Phone 8.1+ | 1.3.3 | Unlimited | Success | Active | admin | Unpublished |
| <input type="checkbox"/> | HR Category: General | Android Tablet | 1.0.0 | Unlimited | Success | Active | admin | Published |
| <input type="checkbox"/> | Auto Category: Cliff Hanger | Android Tablet | 1.0.0 | Unlimited | Success | Active | admin | Published |
| <input type="checkbox"/> | | iPad | 1.0.0 | Unlimited | Success | Active | admin | Published |
| <input type="checkbox"/> | | iPhone | 1.0.0 | Unlimited | Success | Active | admin | Published |

Page {1/2}

The Apps view displays the following columns:

| Columns | Description |
|-----------------|---|
| App Name | <p>The name of app as specified by you while creating and uploading the app to the enterprise store. It is unique. The table is grouped based on the App Name.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Important: Windows Phone 8.x application binary file name must be less than 32 characters. If the name exceeds 31 characters, wrapping process will fail.</p> </div> |
| Platform | Each app may be created for one or more among the four platforms supported. This column shows the platforms for which this specific app is created and uploaded. |
| Version | By default, the latest version of the app is shown. For each platform, typically only one version is shown. The Admin may choose to have older versions of the app to be shown in this table as well. Only the versions displayed here shall be editable when the Admin goes to App Details. |
| Licenses | By default, Unlimited distribution of app license is set. You can restrict license numbers. Available options are Unlimited, 10, 50, 100, and Custom. |
| Wrap Condition | Can be Defunct, Not Initiated, Not Applicable, Aborted, Failed, In Progress and, Success. Appropriate messages are shown for each case. |
| Work Flow State | Displays which state of creation the app is in. Workflow states can only be one of: Draft and Active. |
| Current Owner | Displays the name of the Administrator who owns the app and is therefore able to make changes to its state/status |
| Publish Status | Indicates whether the App is ready for usage or not. If the App is published, it is ready for distribution, else it is not. Can only have 2 statuses - Published and Unpublished |

You can scroll the list view through **Previous** and the **Next** buttons.

Important: For app icons, images only in .png format are supported.

Important: Binaries or any file that is uploaded to portal should not have spaces in a file name.

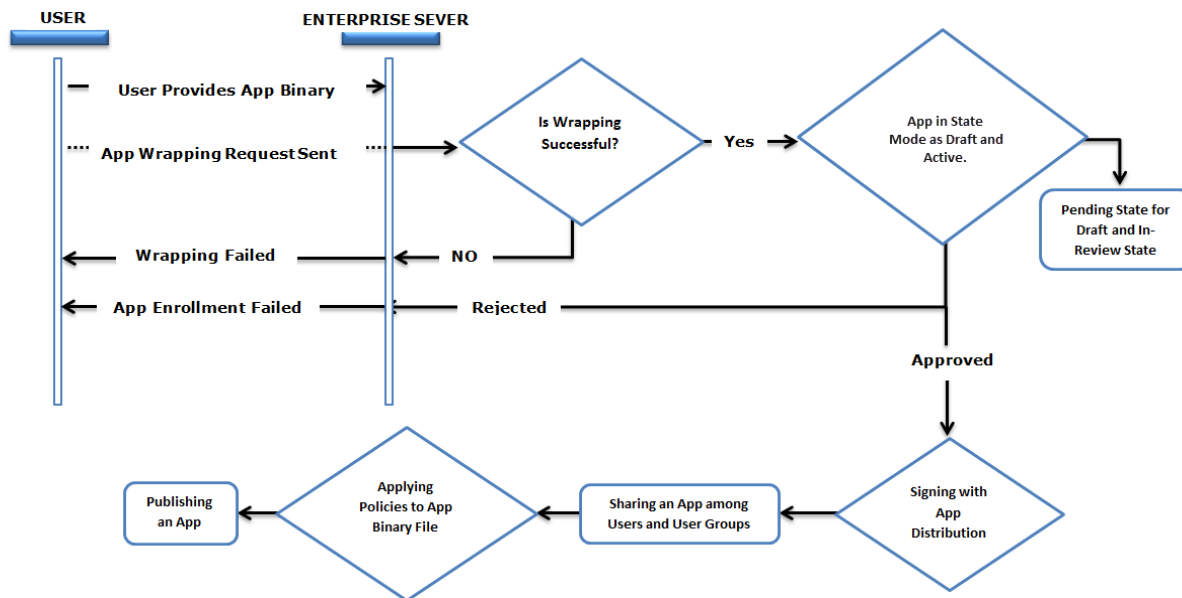
You can perform the following activities from the **Enterprise Apps List** page:

- [Creating a New Enterprise App](#)
- [Publishing an App](#)
- [Searching for Enterprise Apps](#)
- [Updating Enterprise App Details](#)
- [Upgrading Enterprise App Details](#)
- [Adding a New Platform](#)
- [Updating Published Apps](#)
- [Unpublishing an App](#)
- [Deleting an Enterprise App](#)

10.6.1 Creating a New Enterprise App

You can add a new enterprise application to the system from the Enterprise App List page.

Important: Web Browser apps are not supported as Enterprise apps.



The above flow-chart is a simplified depiction of adding a new app to the system.

The **Submit New App** window includes five steps to submit a new app to MAM:

- [Step 1: App Basics](#)
- [Step 2: App Details](#)
- [Step 3: Signing and Targeting](#)
- [Step 4: App Specifics](#)
- [Step 5: Approve and Confirm](#)

10.6.1.1 Step 1: App Basics

To add a new app, follow these steps:

1. To open the **Submit New App** window, click the **+ New App** button next to the **Enterprise Apps List** label at the top of the page.

Important: When you create an app using the graphics intensive User Interface (UI), then you may find that the certain UI elements are missing. To overcome this issue, you need to add the value as `android:hardwareAccelerated="true"` in the application tag of the `AndroidManifest` file. The other option is **Phone Settings > Developer Options > enable Force GPU rendering**. For more information, refer to developer.android.com> dev-options and developer.android.com > graphics

Enterprise Apps

+ New Enterprise App

2. The **Submit New App** window appears. Enter the following details in the App Basics, under Step 1.

The screenshot shows a web-based wizard titled "Submit New App" with five steps: Step 1 (App Basics), Step 2 (App Details), Step 3 (Signing & Targeting), Step 4 (Apps Specifics), and Step 5 (Approve & Confirm). Step 1 is currently active. The "App Basics" section contains the following fields:

- Platforms Supported:** A text input field.
- App Name:** A text input field with a blue border.
- App Description:** A large text area.
- Category:** A dropdown menu with "Select Category" as the placeholder.
- Created By:** A text field containing "Admin".
- App Icon on Console (Size:78x78):** A button with a plus sign and the text "+ Add".

A "Next Step >>" button is located at the bottom right of the form.

a. **Platform Supported:** Select the platform(s) for which the app is created. The following are the platforms supported: iOS phones, iPads, Android phones, Android Tablets, and Windows Phone 8.1. Native apps and web apps are supported. Based on this choice, the necessary binaries and other details must be provided for each platform supported.

b. **App Name:** Enter a valid name for the app.

When you create an enterprise application, ensure that you give it a unique name that clearly describes its purpose, for example, **Kony Financial Advisor**.

- c. **App Description:** Enter a brief description of the app. The description should accurately describe the features and functionality of your app.
- d. **Category:** Select the category that best describes your app. For example, select **Financial** category for the app, **Kony Financial Advisor**.
Category list is pre-populated from the list of categories added to the system. You can update the list of categories from the App Management > [Categories](#) section.
- e. **Created By:** This field populates automatically with the name of the administrator who added a new app.
- f. **App icon on Console:** Click the **+Add** button to add an app icon.
The icon size should be 78x78 pixels and file format should be .png. This icon is shown on the management console and self service console only. This is not shown on the device.

3. Click the **Next Step** button to open **Step 2** window.

Note: This action checks that all the mandatory fields are entered and are in compliance with expectations, else it provides appropriate errors. Admin is required to clear out all errors and only then can proceed to the next step.

10.6.1.2 Step 2: App Details

The App Details pane allows you to either upload the binary for the application being listed or provide a binary URL for the same.

Important: You can upload your own mobile provision files for child apps to use. If you use a provisioning profile with a bundle ID com.xxx.containerapp, wrapping will fail. Ensure that your child app bundle ID does not contain the text containerapp.

Submit New App

Step 1 App Basics | **Step 2 App Details** | Step 3 Signing & Targeting | Step 4 Apps Specifics | Step 5 Approve & Confirm

App Details

iPhone iPad Android Android Tablet Windows Phone 8.1+

App Version

Select Mode Upload Binary Add Binary URL

Binary Files

<< Back Cancel Next Step >>

You can provide APP Details for in two ways (for iOS, Android and Windows) in the **Select Mode**:

The App Details page is different for a Web app. Click [here](#) to see the Web app App Details page.

Important: Wrapping and signing will fail for windows phone applications which contain **xap** or **app** in the apps file name. For example, if the windows phone application is named as **hrapp.xap** or **hrxap.xap** Wrapping and signing for the application fails. If you rename the file and ensure that app and xap are not part of the new name, app submission will be successful.

Important: BLOB (data type) is not supported to create a database (column) in the app if the app is intended to be wrapped over EMM for Wrap/Sign mode. Kony recommends you to use the TEXT data type which can be used by converting BLOB data to Base64 string.

Note: Wrapping/Signing is not supported for Android applications that are built using the Kotlin programming language.

- Upload Binary
- Add Binary URL

1. **App Version:** Enter the version of the app.

App versions can be described in the x.x.x format. For example, 9.2.1060. An app version cannot be x.x.x.x, such as 1.2.5.2.

2. **Upload Binary:** This can be done in 2 ways:

- Dragging and dropping files into the Drag and Drop area.
- Clicking on the **+Add** button and choosing the appropriate files.

Upload Binary property is used to upload the binary from a file path. This allows Admin to Wrap and Sign and therefore assign policies and more control over the app. Policy can be injected dynamically and custom applied to targets.

- a. Click the **+ Add** button to browse the location of Binary File.
- b. Select the file, and open it.

A binary file contains any type of data, encoded in binary form for computer storage and processing purposes.

The Binary file is added with name and size details in **Drag and Drop Files Here** field. Once the file is added, the **Upload** button is activated.

Important: A .plist file must accompany the .ipa for iOS applications. We recommend that you provide the .plist file and .png files. If you do not provide these files, while uploading binaries for iOS only, the system generates .plist files automatically and then displays the **Bundle Identifier** in the **Step 3 > Signing & Targeting**. For more details, refer to [Auto-generating .plist Files while Submitting an App](#)

- c. Click the **Upload** button.

Only a link is provided in this process. When the device attempts to install the app, the device is sent to the link specified here to source the binary.

Important: In EMM 2.5, enhanced security enables app binaries for iOS and Android platforms. Modified binaries (of enterprise store or other enterprise apps) are detected and not run. This enhanced security will protect devices from programmed threats and information leaks.

Note: If you upload any Android .apk file with .jar files in it, when you upload that .apk file in Kony Management Suite, it will result in a runtime crash of the Android application.

Before you submit any .apk file to Kony Management suite, delete any .jar files in the .apk file.

To check if you have any .jar files in your .apk, open the .apk with an archive opening app (for example, Winzip or 7-zip) and then delete any .jar files from the .apk file.

3. Add Binary URL

- a. Click **Add Binary URL**. The Binary URL, Size (in KB), and Submitted links fields appear.
- b. Enter the following details:
 - **Binary URL**: Enter the URL.
 - **Size in KB**: Enter the binary file size.

Note: When a Binary URL is added, it is important to remember that the application cannot be wrapped and policies cannot be added to the binary URL as apps can only be signed. Only app distribution can be managed for apps uploaded through this method.

4. Click the **Next Step** button to navigate to **Step 3**

Click the **Back** button to navigate to **Step 1**

Web App App Details

When you choose a platform as a web app, then you see the following screen in the App Details page.

Submit New App

Step 1 App Basics | **Step 2 App Details** | Step 3 Signing & Targeting | Step 4 Apps Specifics | Step 5 Approve & Confirm

App Details

iPhone ★ | Android ★ | Webapp

Platforms Supported

- Android
- Android Tablet
- iPhone
- iPad
- Windows Phone 8.1+

Android URL

Android Tablet URL

iPhone URL

iPad URL

Windows Phone 8.1+ URL

<< Back | Next Step >>

- **Platforms Supported:** You can select the platform for which you want to add the web app. Based on the type of platform you select, more fields appear below the **Platforms Supported** field.
- **Android URL:** Enter the Android phone web app URL.
- **Android Tablet URL:** Enter the Android tablet web app URL.
- **iPhone URL:** Enter the iPhone web app URL.
- **iPad URL:** Enter the iPad web app URL.
- **Windows Phone 8.1 + URL:** Enter the Windows Phone 8.1 web app URL.

Auto-generating .plist Files for iOS While Submitting an App

For iOS, if you do not upload a `.plist` file and `.png` files, the system generates `.plist` files automatically while submitting an app.

The `.plist` file includes an `.ipa` file and icons submitted by a user. While uploading binaries for iOS, the system displays the **Bundle Identifier** in the **Step 3 > Signing & Targeting** based on the different scenarios.

The following table details bundle IDs for different scenarios:

| No. | If you upload | The system displays |
|-----|--|--|
| 1 | A <code>.plist</code> file and a Mobileprovision adhoc certificate <mobileprovision> | Bundle Identifier as <com.kone.test.myapp> The priority for bundle id is given from <mobileprovision> file. For example, if a <code>.plist</code> file has tag as <com.kone.myGoogle> and mobileprovision file has tag as <com.kone.test.myapp>, then the bundle id is <com.kone.test.myapp> |
| 2 | A <code>.plist</code> file, a MobileProvision adhoc certificate, and a wildcard certificate, | Bundle Identifier as <com.kone.test.myGoogle> For example, if <code>.plist</code> file has tag as <com.kone.myGoogle> and mobileprovision file has tag as <com.kone.test.*>, then the bundle id is <com.kone.test.myGoogle>. The "<myGoogle>" is taken from <code>.plist</code> file. |

| No. | If you upload | The system displays |
|-----|--|--|
| 3 | Only an .ipa file, | Bundle Identifier as: Global wildcard mobile provision <com.kone.> + Text box appears User needs to fill in the value in the text box. The text fields supports alphanumeric characters, but no special characters. For example, <com.kone.Test>; <com.kone.x.Test> |
| 4 | Only a .ipa file, and a wildcard mobileprovision file, | Bundle Identifier as user provided wildcard mobileprovision <com.kone.xyz.> and a Text box. User needs to enter the value in the text box after the dot(.). |
| 5 | Only a .ipa file, and an ad hoc mobileprovision file, | Bundle Identifier as per ad hoc mobileprovision. For example, <com.kone.xyz.Test> |

Important: If you upload a mobile-provision profile that is different from the profile uploaded earlier, the system throws a bundle ID mismatch error.

Error messages while uploading an expired profile

If an expired profile is uploaded, the system displays mobile-provision expired error message as shown below:

App Details

iPad

Missing optional file of type: image,.plist

App Version

Select Mode Upload Binary Add Binary URL

Binary Files

| | | | |
|-------------------------------------|---------|--|----------------------------------|
| KonyEMMDistribution.mobileprovision | 7.36 KB | .mobileprovision has exceeded its validity period (valid till Jan 7, 2013) | <input type="button" value="🗑"/> |
| JavaConnectorApp.ipa | 8.89 MB | | <input type="button" value="🗑"/> |

Generating .ipa and .plist Files

To generate .ipa and .plist files through Xcode, follow these steps:

1. Once you extract the `kar` file, open the Xcode project.
2. Select the option **Product > Archive**.
3. Select the option **Window > Organizer**, and select the application, and select the option **Distribute**.
4. Select the **Save for enterprise or Adoc deployment** option, and export the file.
5. While saving the .ipa, select the option **Save for Enterprise Distribution**, and then click **Save**.

Once the file is saved, the system creates .ipa and .plist files. You can upload both the files in EMM console while creating the new application.

10.6.1.3 Step 3: Signing and Targeting

The App Signing window includes three sections:

- Signing and Wrapping
- iOS Properties (for an iOS app)
- Custom Attributes
- Targeting

Each of these actions must be done across all the platforms supported.

Only those apps whose binaries are uploaded can be wrapped. Apps for which Binary URLs are provided cannot be wrapped. If an app cannot be wrapped or is already wrapped, Administrator can choose to only sign.

Important: For iOS Different team identifiers (app id prefix): In case where you upload an app generated by a third party, wrap and sign may fail. This is because the team identifier of the third party (in the ipa) is different than your team identifier (in the certificates that you procured from Apple). The information about your team identifier is part of the certificates that you have uploaded in the certificates tab of the Application settings page of Kony management admin console.

The screenshot shows the 'Submit New App' wizard in the Kony Management Console. The wizard is titled 'Submit New App' and has five steps: Step 1 (App Basics), Step 2 (App Details), Step 3 (Signing & Targeting), Step 4 (Apps Specifics), and Step 5 (Approve & Confirm). Step 3 is currently active and highlighted in orange. The 'Signing & Targeting' section is expanded, showing options for 'iPhone' and 'Android'. Below this, there is a 'Targeting' section with two buttons: '+ Manage groups' and '+ Manage users'. A text box below these buttons displays 'Group / User' and 'No groups/users targeted'. At the bottom of the wizard, there are two buttons: '<< Back' and 'Next Step >>'.

Signing and Wrapping

- **Bundle Identifier (iOS) or Package Name (Android):** While uploading binaries for iOS, the system displays **Bundle Identifier** in the **Step 3 > Signing & Targeting** based on the different

scenarios. For more details, refer to [Auto-generating .plist Files while Submitting an App](#)

Signing Rule: There are two options available: **Wrap and Sign** or **Only Sign**. As described in the [App Details](#) section, Wrap and Sign can only be used for apps whose binary is uploaded. For all other apps, Only Sign is used.

- **Only Sign:** This is used for apps that are already wrapped or cannot be wrapped. This is the only choice if a binary URL was provided.
- **Wrap and Sign:** This is used for any new app whose binary has been uploaded. If you select Wrap and Sign, a new option **Allow Direct Launch** is enabled.

Note: For Windows Phone 8.x apps, only C# XAML based apps are supported for wrapping and signing.

Windows Phone 8.x app wrapping

For Windows Phone 8.x devices, the following are the limitations for App wrapping.

- If admin uploads other than C# XAML app, although that will be considered for “Wrap & Sign” option but does not guarantee the successful wrapping. Policies may or may not work for these apps if wrapped successfully.
- Not all the policies will work for web view. See the table below.

| WebView Policy | Windows phone 8.x (XAP) | Windows phone 8.x (APPX) |
|------------------|-------------------------|--------------------------|
| Copy paste | No | No |
| Document sharing | No | No |
| Network | Yes | Yes |
| Phone Features | Yes | No |

- **Allow Direct Launch:** This feature is enabled when the **Signing Rule** field is configured to **Wrap and Sign**. By default, this option is configured to **No**. Select **Yes** to enable the app to launch directly on the device outside the enterprise store.

You can configure the Allow Direct Launch feature when you create, update, and upgrade an app, and or when you add a new platform. Publish an app if you make any changes to the app. Changes made to the app will reflect after the app is republished.

- **Allow SSO:** Configuring this to **Yes** enables Open ID 2.0 single sign on authentication for the enterprise app.

If an enterprise app and the enterprise store are authenticated with the same OpenID 2.0 server, logging into the enterprise store automatically authenticates the user to use the enterprise app. Suppose the enterprise store does not have OpenID 2.0 authentication enabled, but the enterprise app has OpenID 2.0 authentication. When you open the enterprise app in the enterprise store, you need to authenticate with your OpenID 2.0 login credentials to open the enterprise app.

Note: If you want the Enterprise store to be able to share user access information (such as cookies, SSL certs, etc.) with an app, enable SSO.

- **Enable Two-way SSL:** The SSL certificate is used to contact any server resource inside a customer's network that requires mutual authentication. Configuring this to **Yes** allows the client and the server to authorize each other so both parties are assured of each others identities. This works only for Android.

Note: Kony Management does not support SCEP Two-way SSL for iOS.

iOS Properties



The screenshot shows a configuration window titled "iOS Properties". It contains two main sections: "Assigned VPN" with a dropdown menu currently set to "VPN 1", and "Managed App Configuration" which includes a "Configure" button and a lock icon next to the text "iOS 7+".

Assigned VPN

Only VPNs enabled to be Per App VPN are displayed in the **Assigned VPN** drop-down list. For more details, refer to [Assigning Per App VPN for iOS](#). Per App VPNs can be assigned to Enterprise apps while creating apps, updating apps, upgrading apps, or adding new platforms. Per App VPNs can be assigned only to Required Apps. Only one Per App VPN can be assigned for each app. To assign a Per App VPN to an enterprise app, select one of the Per App VPNs from the **Assigned VPN** drop-down list.

Managed App Configuration

If an app is built according to standards for iOS 7+ and later, the Managed App Configuration feature allows an administrator to view some of the properties that can be configured. For example, background color of the app or font of the app could be changed. An app developer must define the required keys and values, and these details must be shared with the EMM administrator.

To configure the Managed App Configuration, follow these steps:

1. Click the **Configure** button. The AppName Configuration dialog appears.
2. In the AppName Configuration dialog, provide the details for Keys and Values.

| Key | Value | |
|------------------------------------|----------------------|--|
| <input type="text" value="Key 1"/> | <input type="text"/> | <input type="button" value="Add"/> <input type="button" value="Remove"/> |
| <input type="text" value="Key 2"/> | <input type="text"/> | <input type="button" value="Add"/> <input type="button" value="Remove"/> |
| <input type="text" value="Key 3"/> | <input type="text"/> | <input type="button" value="Add"/> <input type="button" value="Remove"/> |
| <input type="text" value="Key 4"/> | <input type="text"/> | <input type="button" value="Add"/> <input type="button" value="Remove"/> |

3. Click **Add**. The system creates a new row. You can also delete a row by clicking **Remove**.
4. Click **Save** to save the configuration.

Custom Attributes

You can assign any of your custom attributes (configured in the Settings section) to your app. Select the custom attribute set from the **Custom Attribute Configuration** list.




Targeting

Targeting makes apps accessible to users and applies policies to the apps. Targeting also determines whether access to the app is mandatory for any user or group. On devices, only targeted users are shown the app in their enterprise store in the Store tab of the Kony EMM enterprise store. Therefore, only targeted users can download the app and install it on their devices.

Note: Super administrators can target enterprise apps to any user, group, or domain. Administrators with limited access can only target users, groups, and domains they have access to.

Targeting

+ Manage groups
+ Manage users

| <input type="checkbox"/> | Group / User | Mandatory | Policy | Policy Priority |
|--------------------------|---|--------------------------|---|-----------------|
| <input type="checkbox"/> | Kobe  (domain1.kony.com) | <input type="checkbox"/> | None ▼ | 0 |
| <input type="checkbox"/> | Kobe  (domain2.kony.com) | <input type="checkbox"/> | None ▼ | 0 |
| <input type="checkbox"/> | Kobe  | <input type="checkbox"/> | None ▼ | 0 |

Apps can be targeted to individual users or groups associated with domains. Take the following steps:

1. Click **Manage Users**, and select the targeted users for the app.
2. Click **Manage Groups**, and select the targeted groups. The domain of the users or groups is always shown here.
3. A list of users associated with domains appear. You can search for the required user by entering a partial or complete user name in the Search field. To assign a user, click the right single arrow icon. To assign the complete user list, click the right double arrow icon.
4. Click **Target Users**. The selected user detail appears in the Group/User column. You assign a policy to the selected user from the drop-down list available under Policy column.
5. To make the assigned policy mandatory, select the check box available under Mandatory column.

6. Click the **Next Step** button to navigate to [Step 4: Apps Specifics](#).

Click the **Back** button to navigate to [Step 2: App Details](#).

10.6.1.4 Step 4: App Specifics

In the App Specifics window, you can upload application-specific files like icons, screenshots, user guides. Select the required files for the fields.

The screenshot shows the 'Submit New App' interface, specifically the 'Step 4: Apps Specifics' window. The interface is divided into several sections:

- Progress Bar:** Located at the top, it shows five steps: Step 1 (App Basics), Step 2 (App Details), Step 3 (Signing & Targeting), Step 4 (Apps Specifics, highlighted in orange), and Step 5 (Approve & Confirm).
- App Specifics Section:** This section is titled 'App Specifics' and contains several fields for uploading files:
 - Application Icon on Device (Size: 84x84):** A field with a small image of a dog's face.
 - App Screenshot(s) (320x480):** A field with four placeholder boxes, each containing a '+ Add' button.
 - App Guidebook(s):** A field with a '+ Add' button and a text box below it containing the text 'Click add or Drag & Drop here'.
- Navigation:** At the bottom of the window, there are three buttons: '<< Back', 'Cancel', and 'Next Step >>'.

1. **Application Icon on Device:** Click the **+Add** button to find the image in your system to add.

Select the image and click Open. The image appears in the **Application Icon on Device** section. Provide an appropriate and original PNG image of high quality with a size of 84X84 pixels.

2. **App Screenshot(s):** Select the screenshots of your app. These screenshots are displayed for your app. Click the **+Add** button to find the image in your system to add. Select the image and click Open. The image appears in the **App Screenshots** section.



The first screenshot that you upload appears on your app page. You can upload four supplementary screenshots. All subsequent screenshots appear in the order in which they were uploaded. Provide an appropriate and original PNG image of high quality with a size of 320x48 pixels.

3. **App Guidebook(s):** Click the **+Add** button to find the guidebook in your system to add. Select it and click the Upload button. The guidebook and its size appear in the Drag and Drop Files Here box.

Guidebooks are documents to help a user to understand how to use the application being uploaded. They appear along with the app in the Enterprise Store. The guidebook can be a plain text file, in rich text format or a PDF.

4. Click the **Next** button to navigate to [Step 5: Approve and Confirm](#)

Click the **Back** button to navigate to [Step 3: Signing & Targeting](#).

10.6.1.5 Step 5: Approve and Confirm

The **Confirm and Approve** window is the final step. A summary of all choices made are displayed to the administrator. The administrator can either **Submit** or **Cancel** the app.

Submit New App

Step 1
App Basics
Step 2
App Details
Step 3
Signing & Targeting
Step 4
Apps Specifics
Step 5
Approve & Confirm

Confirm & Approve

App Name My_Sample_App

App Version 1.4

Category EMM_Automation

Publisher Aravind Gubba

iPhone
iPad
Android
Android Tablet
Windows Phone 8.1+

Binary Files myspace.android.apk

Signing Rule Wrap and Sign

Bundle Identifier com.myspace.android

| Group / User | Mandatory | Policy | Policy Priority |
|---------------------|-----------|--------------|-----------------|
| AdminGrp (AdminGrp) | Yes | ipad2 policy | 3 |

<< Back
Cancel
Submit App

- Once you confirm the details, click the **Submit App** button to register the new app. The system displays the confirmation message: App created. Click **OK** to continue.

The newly created app appears in the list view. The current Workflow State is **Draft**, and the Publish Status is **Unpublished**. The current Wrap Condition is In-Progress, which changes to Success.

| App Name | Platform | Version | Licenses | Wrap Condition | Workflow State | Current Owner | Publish Status |
|--|---|------------------------------------|--|--------------------------------------|---|--|---|
| <input type="text" value="Search Apps"/> | <input type="text" value="All Platforms"/> | | | <input type="text" value="All"/> | <input type="text" value="All States"/> | <input type="text" value="Search Owner"/> | <input type="text" value="All Statuses"/> |
| <input checked="" type="checkbox"/> My_Sample_App Category: EMM_Automation | <input checked="" type="checkbox"/> Android | <input type="text" value="1.4.0"/> | <input type="text" value="Unlimited"/> | <input type="text" value="Success"/> | <input checked="" type="text" value="Draft"/> | <input type="text" value="Aravind Gubba"/> | <input checked="" type="text" value="Unpublished"/> |

Click the **Cancel** button to close the window.

10.6.2 Licenses

You can restrict distribution of an app through the Enterprise App licenses feature.

The Licenses page displays the following.

Licenses - Testdoc, 1.0.0 (Android)

Total Licenses

Note Total Licenses should be greater than or equal to No. of licenses consumed + No. of not-installed mandatory users.

Licenses Consumed 0
 Licenses Available 10
 Total Mandatory Users 0 (Installed: 0, Not-installed: 0)

Consumed Users

Displaying 0 - 0 of 0 - Display

| <input type="checkbox"/> | Display Name | User ID | Source | Status |
|--------------------------|---|---|--|--------|
| | <input type="text" value="Search User Display Name"/> | <input type="text" value="Search User ID"/> | <input type="text" value="All Domains"/> | |
| No results found | | | | |

Page {1/1}

- **Total Licenses:** Displays a list from which you can choose the number of licenses the application can have. Available options are Unlimited, 10, 50, 100, and Custom.
- **Licenses Consumed:** Displays the number of licenses consumed.
- **Licenses Available:** Displays the number of licenses available.

Important: For Windows Phone 8.1 devices, users can install an app even after the number of licenses permitted are consumed. However, the user cannot use the app, and a command to remove the app is sent to the device.

- **Total Mandatory Users:** Displays details of licenses consumed by mandatory users and remaining licenses.
- **Consumed Users:** This section displays details on users who consumed licenses.
 - **Display Name:** Display name of the user using the license.
 - **User ID:** User ID of the user using the license.
 - **Source:** Domain details of the user using the license.
 - **Status:** Status of the application whether it is installed or not.
- **Recall Now:** You can use this button to recall a license.
- **Previous:** Clicking this button takes you to the previous page (if it exists).
- **Next:** Clicking this button takes you to the next page (if it exists).

10.6.3 Publishing an App

Only after publication an app becomes available at an App Store and a User can view and download it from a device or Self Service Console. Unpublished apps are visible to Admin only. Once an app is created, it is displayed in the list view. As a prerequisite, to make changes in the **State** and the **Status** of an app, you should own that app.

App State

By default, an app appears as a draft in the list view. This draft is submitted for review to the administrator. After review, you can convert the submitted state into Active. The following charts describe about the App State Workflow:

See the table below for a description of the app states.

| State Name | Description |
|------------|--|
| Draft | Appears as the first state for your app. |


| State Name | Description |
|------------|---|
| Active | Appears when the binary has passed review and approved by an administrator and is active. |

App Status

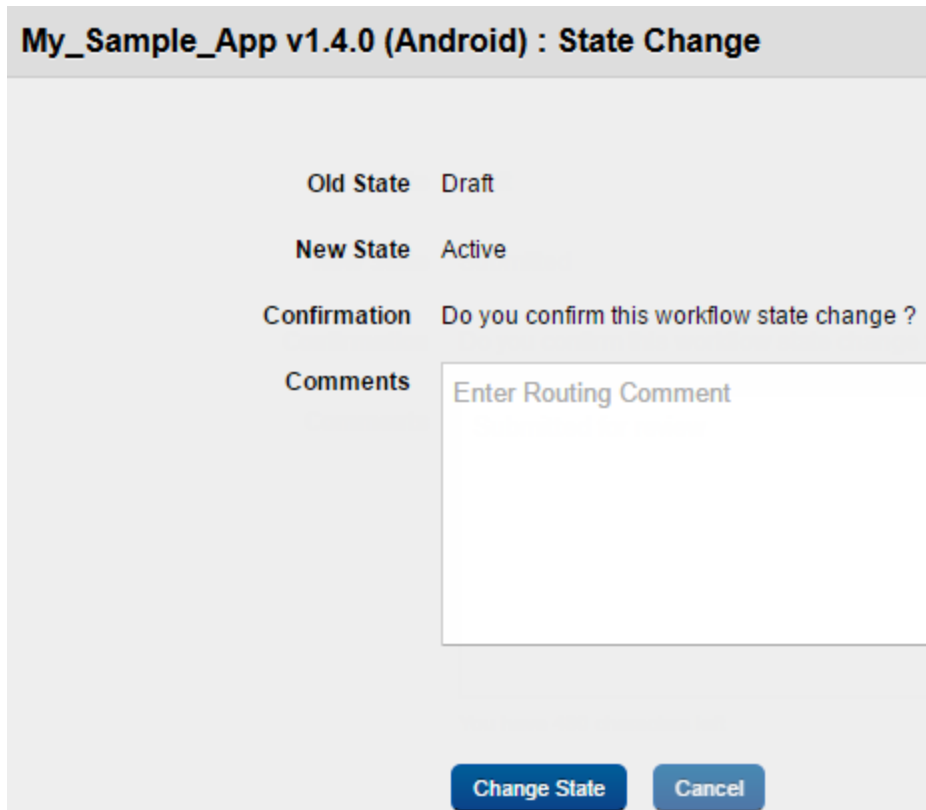
By default an app has Unpublished status in list view. You can change the status from Unpublished to Published. You cannot delete a published app. To delete a published app, first you need to revert the status as unpublished.

To publish an app, follow these steps:

1. A newly created app appears in **Draft** state and the default Status is **Unpublished**. Click the State drop-down list to change the State from Draft to Submitted.

| Search Apps | | All Platforms | | All | All States | Search Owner | All Statuses |
|--------------------------|--|---------------|-------|-----------|------------|---------------|--------------|
| <input type="checkbox"/> |  My_Sample_App Category: EMM_Automation | Android | 1.4.0 | Unlimited | Success | Aravind Gubba | Unpublished |

The **State Change** window appears.



My_Sample_App v1.4.0 (Android) : State Change

Old State Draft

New State Active

Confirmation Do you confirm this workflow state change ?

Comments Enter Routing Comment

Change State **Cancel**

2. Enter an appropriate comment in the **Comments** text box.
3. Click the **Change State** button. In the confirmation message that appears, click **OK** to proceed.

The Workflow State changes to **Active** in the list view.

4. To publish the app, select the **Publish** option from the drop-down list under Publish Status column. The **State Change** window appears.
5. Enter an appropriate comment in the **Comments** text box. Click the Publish button to proceed. The system displays the confirmation message stating that published App is now available in Store. Click **OK** to proceed.

10.6.4 Searching for Enterprise Apps

You can search a desired app through search filters available. You can apply a single or a combination of search filters to define the search criteria and get the refined outcome.

Important: When you search for an app, all apps and categories which contain your search terms (including numbers) in their name, or version number will appear in the search results.

To search an app, follow these steps:

| <input type="checkbox"/> | App Name | Platform | Version | Licenses | Wrap Condition | Workflow State | Current Owner | Publish Status |
|--------------------------|--|--|---------|----------|----------------------------------|---|---|---|
| | <input type="text" value="Search Apps"/> | <input type="text" value="All Platforms"/> | | | <input type="text" value="All"/> | <input type="text" value="All States"/> | <input type="text" value="Search Owner"/> | <input type="text" value="All Statuses"/> |

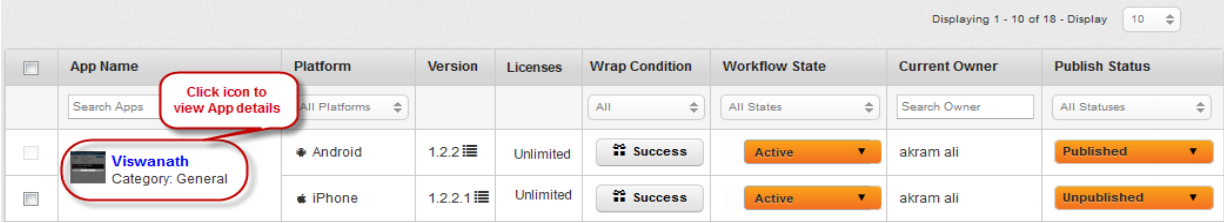
1. Enter or select the following search criteria:
 - a. **App Name:** Enter partial or complete name of the app in the **Search Apps** field.
 - b. **Platform:** Select the required platform from the drop-down list. By default, it is set to All Platforms. You can modify it to iPhone, iPad, Android and Android Tablet.
 - c. **Wrap/Sign Condition:** Select the required Wrap condition from the drop down menu. By default, it is set to **Success**. You can modify to All or Failed.
 - d. **State:** Select the required State from the drop-down menu. By default, it is set to **All States**. You can modify to Draft or Active.
 - e. **Current Owner:** Enter the name of the current owner.
 - f. **Status:** Select the current status of the app from the drop-down list. By default, it is set to All Statuses. You can modify to Published or Unpublished.

2. According to your search filters criteria, the list view is updated with respective app details. By default, the list view displays ten apps according to Display settings, which you can modify through Display dropdown list. You can also scroll the list view through **Previous** and the **Next** buttons.

10.6.5 Updating Enterprise App Details

Updating an Enterprise app pertains to modifying the details of the added app. You may need to update app details for specific reasons, for example, you may need to update app name, app category, or app icon on console.

The Status remains Published but the State reverts back to Draft state. After submission, the app moves to Active. You need to publish this app again to reflect the updates. A stale state icon next to the corresponding app version is used to indicate that changes have been made to the definition of the application.



| App Name | Platform | Version | Licenses | Wrap Condition | Workflow State | Current Owner | Publish Status |
|--------------------------------|----------|---------|-----------|----------------|----------------|---------------|----------------|
| Viswanath Category: General | Android | 1.2.2 | Unlimited | Success | Active | akram ali | Published |
| | iPhone | 1.2.2.1 | Unlimited | Success | Active | akram ali | Unpublished |

Click the app name in the list view which you need to update. The App Settings page appears.

After your app has gone through the initial review procedure, you can make changes to your app by editing app-level information. You can update details through following tabs. By default App Settings tab is set to active.

To update an app, follow these steps:

1. **App Name:** In the app name field, your previously chosen name has been repopulated and displays it. If required, update the app name.
2. **App category:** In the app name field, your previously chosen category has been repopulated and displays it. If required, update the app category.
3. **App icon on Device:** In the app icon on console your previously chosen icon has been repopulated and displays it. If required, update the app icon via **+Add** button.
4. **App Icon on Console:** In the app description field your previously written description has been repopulated and displays it. If required, update the app description.
5. Update other tabs if required. For more details, refer to the following:
 - [Creating a New Enterprise App > App Details](#)
 - [Creating a New Enterprise App > Signing and Targeting](#)

- [Creating a New Enterprise App > App Specifics](#)

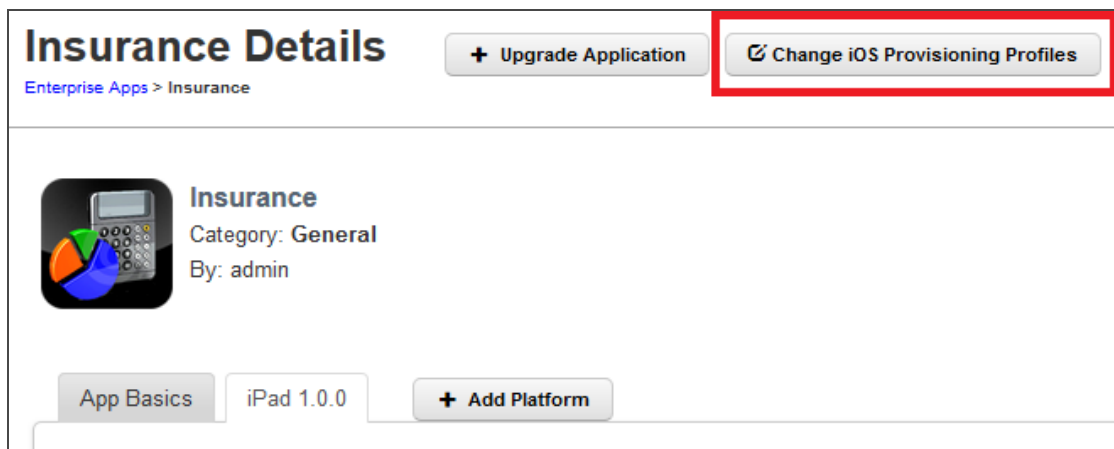
6. Click the **Save and Exit** button to save the updated details. In the confirmation message that appears, click **OK** to continue.

10.6.5.1 Changing iOS Provision Profiles

While editing app details, an administrator can also add or edit iOS mobile-provision profiles.

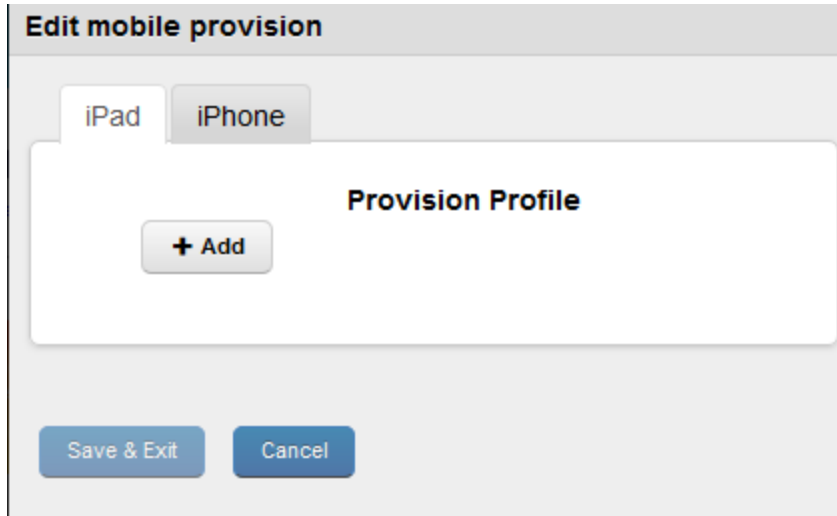
To change mobile-provision profiles, follow these steps:

1. Click the app name in the list view that you need to update. The App Settings page appears.



2. Click the **Change iOS Provisioning Profiles** button next to the Upgrade Application.

The **Change iOS Provisioning Profiles** button is active only for iOS.



The **Edit mobile provision** dialog appears.

3. Click the **+ Add** button to add or modify a profile.
4. Click **Save** to save the changes.

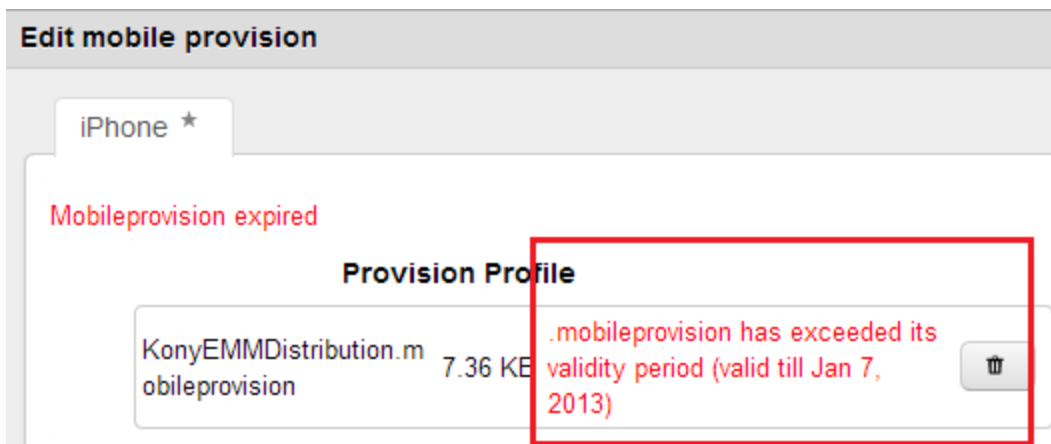
The following tables lists error messages:

| No. | If you upload | If not found, the system displays the follow error message |
|-----|--|--|
| 1 | An adhoc mobile-provision profile, the system validates for a valid bundle ID that is present within the mobile-provision profile. For example, if an app bundle ID is <com.kone.xyz>, the adhoc mobile-provision profile must be <com.kone.xyz>, otherwisethe system displays an error message. | Bundle ID mismatch |

| No. | If you upload | If not found, the system displays the follow error message |
|-----|---|--|
| 2 | A wild mobile-provision profile, the system looks for a new wild mobile-provision profile that has an app bundle ID matching with the provision file. For example, if the app bundle ID is <code><com.kone.x.Test></code> , then the user upload wildcard mobile-provision profile must be <code><com.kone.x.*></code> For example, if the app bundle ID is <code><com.kone.Test></code> , then the user upload wildcard mobile-provision profile must be <code><com.kone.*></code> | Bundle ID mismatch |

Error Message While Editing an Expired Profile:

If an expired profile is edited, the system displays mobile-provision expire error message as shown below:



10.6.6 Upgrading Enterprise App Details

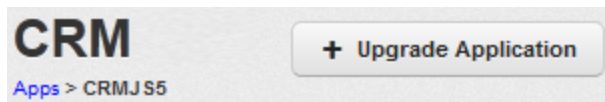
You may wish to upgrade the added application details if new functionality have been added in your app, and binary file is modified etc. This process upgrades the app version.

Important: To upgrade an enterprise app, you must own the latest version of the app and have permissions to upgrade the app.

The Upgrade App window includes five steps to upgrade an app details:

To upgrade an app, follow these steps:

1. To open the **Upgrade App** window, click the ^ **Upgrade Application** button next to the App label on the top of the page.



Upgrade App Window appears.

2. Select the platform to be upgraded and click the **Next** button.

The mechanism of providing the app should not be altered in the Upgrade process.

- If an app is provided with a binary URL, it should be provided with a URL.
- If an app is provided with a binary file, it should be provided with a binary file.

If this is changed, the app becomes unstable.

Upgrade App

Step 1 App Basics | **Step 2 App Details** | Step 3 Signing & Targeting | Step 4 Apps Specifics | Step 5 Approve & Confirm

App Details

iPhone

App Version
current version: 1.0.0.1

Select Mode **Upload Binary**

Binary Files

Click add or Drag & Drop here

<< Back | Cancel | Next Step >>

When you upgrade an app, the **Step no. 2: App Details** window displays the initial selection next to **Select Mode** label.

- If the initial selection was **Add Binary Files**, then the button appears.
 - If it was to provide a **Binary URL**, the Admin must provide a URL.
3. Upload the binary file or add the binary URL. For procedure details, refer [Creating a New Enterprise App > App Details](#)
 4. Sign the application and assign the target user/group. For procedure details, refer [Creating a New Enterprise App > Signing and Targeting](#)

5. Add Specifics by adding a new icon or application image, if required. For procedure details, refer [Creating a New Enterprise App > App Specifics](#)
6. The Confirm and Approve window is the final step. A summary of all the choices made are displayed to the Admin. The admin can then choose to submit the upgraded app or Cancel the same.

Important: For iOS, when an existing enterprise app upgraded and is submitted for signing and wrapping, Kony Management Enterprise Store (previously Launchpad) will be re-wrapped. The device users will be prompted to update their present enterprise store to the new version.

While upgrading apps that are signed only must continue as signed only. Similarly, while upgrading apps that are wrapped and signed must continue as wrapped and signed-only. Add binary apps should be upgraded as add binary only. Other than the above combinations Enterprise apps should not be allowed.

Note: On iOS 7.0, whenever a mandatory app is upgraded, the app is installed on device silently.

Note: On SAFE enabled devices, whenever a mandatory app is upgraded, the app is installed on device silently.

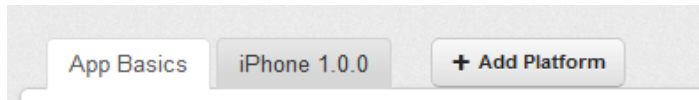
10.6.7 Adding a New Platform

You may wish to add new platforms for your app. This process adds only unsupported platforms. You cannot add an existing platform.

This whole process involves five steps:

To add a new platform, follow these steps:

1. To open Add Platform window, click the **+Add Platform** button next to the **App Basics** tab.



Add Platform window appears.

2. Select the platform to be upgraded and click the **Next** button.
3. Upload the binary file or add the binary URL. For procedure details, refer [Creating a New Enterprise App > App Details](#)
4. Sign the application and assign the target user/group. For procedure details, refer [Creating a New Enterprise App > Signing and Targeting](#)
5. Add Specifics by adding a new icon or application image, if required. For procedure details, refer [Creating a New Enterprise App > App Specifics](#)
6. The Confirm and Approve window is the final step. A summary of all the choices made are displayed to the Admin. The admin can then choose to submit the updated app or Cancel the same.

10.6.8 Updating Published Apps

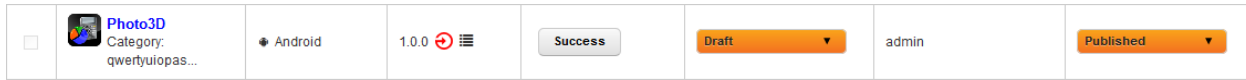
If there are changes to the App definition, you may require updating the published Apps. After updating a published App, the status remains Published but it undergoes a change of state to Draft state. To validate the carried out updates, you need to republish the App.

| App Name | Platform | Version | Wrap Condition | Workflow State | Current Owner | Publish Status |
|---------------------------------------|---------------|---------|----------------|----------------|---------------|----------------|
| Search Apps | All Platforms | | All | All States | Search Owner | All Statuses |
| Viswanath Category: General | Android | 1.2.2 | | Draft | akram ali | Published |
| | iPhone | 1.2.2.1 | | Active | akram ali | Unpublished |

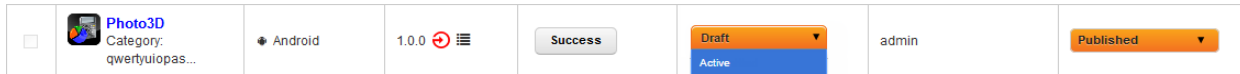
A stale state icon next to the corresponding App Version is used to indicate that changes have been made to the definition of the App.

The state must be changed to Approved and published again for the changes to take effect.

To publish the App again, follow these steps:



The current State is **Draft** and the current Status is **Published**.



1. Select the State as **Submitted** from the drop down menu.

State Change window appears.

Photo3D v1.0.0 (Android) : State Change

Old State Draft

New State Active

Confirmation Do you confirm this workflow state change ?

Comments

2. Enter a valid reason for state change in the **Comments** text box.
3. Click the **Change State** button to submit the state change details. The System displays the confirmation message: Successfully changed state. Click **OK** to proceed. The State changes to **Active**.

The current State is Approved and the current Status is Published.

4. Select the Status as Republish from the drop-down menu.
5. The System displays the Success message: Successfully published. Previous published information about App successfully rewritten. Click **OK** to proceed.




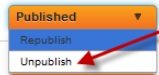

The Stale icon next to app version is removed. The current State is **Active** and the current Status is **Published**.

10.6.9 Unpublishing an App

To deactivate an Application, the Administrator should unpublish the same. Unpublishing an application signifies that:

- The App is no longer displayed in the App store.
- All App data is removed.
- The App is marked to be deleted from the device.
- The App and its details can be deleted from the MAM console.

To unpublish the App, follow these steps:

| | | | | | | | |
|--------------------------|---|----------------|---|---------|------------|-------|---|
| <input type="checkbox"/> |  Camwifi Category: Finance | Android | 1.5.0   | Success | Approved ▼ | admin |  |
| <input type="checkbox"/> | | Android Tablet | 1.5.0  | Success | Draft ▼ | admin | |

1. Select the status as Unpublish from the drop-down menu.

Unpublish window appears.

Camwifi v1.5.0 (Android) : UnPublish

Confirmation Do you want to unpublish this App ?
App will not be available in Store after unpublish.

Comments

2. Enter a valid comment.
3. Click the **Unpublish** button to proceed. In the confirmation message that appears, click OK to return to the main page.

| | | | | | | | |
|--------------------------|-------------------------------------|----------------|-------|---------|----------|-------|-------------|
| <input type="checkbox"/> | Camwifi Category: Finance | Android | 1.5.0 | Success | Approved | admin | Unpublished |
| <input type="checkbox"/> | | Android Tablet | 1.5.0 | Success | Draft | admin | Unpublished |

4. The App Status changes to **Unpublished**.

The Unpublished status can be reverted to Published.

10.6.10 Deleting an App

If an app is no longer required, you can delete it.

| | | | | | | | | |
|--------------------------|---|--------|-------|---------|-----------|-----------------|-----|-----------|
| <input type="checkbox"/> | Wholesale CRM Category: Finance | iPad | 5.0.2 | Success | Submitted | Johnathon Davis | Own | Published |
| <input type="checkbox"/> | Market Watch Category: Finance | iPhone | 4.0.2 | Success | Submitted | Steven Jenkins | | Published |

Select Checkbox and click Delete Button Page {3/92}

To delete an app, follow these steps:

1. Select the app through check box next to it in the grid view.
2. Click **Delete** button. The selected app is deleted from the list view. You can delete only unpublished apps. If you try to delete a published app, system displays an error message stating that only unpublished apps can be deleted. Once you delete an app, it is removed from the list view.

11. Content Management

Mobile content management is a key component of enterprise mobility management framework, which enables targeting content and applying policies to users and groups. Content is organized in folders and these folders are available to users through content policies targeting individual users or groups.

This section provides information on management console where an administrator uploads and controls all content for the enterprise. Information on a user uploading and managing their content is provided in the [Self Service console](#) section.

In EMM 3.0, users cannot edit the content. EMM server does not synchronize from the device. All content on the device is read only.

Content management allows policies to be applied on content. Content policies apply only to iOS devices, for Android and Windows devices, policies are not applicable. Examples of content policies include - control editing, prevent sharing through email or social media channels, prevent copy/paste, expire documents and so on. In Android and Windows, content does not have any designated document reader. Content on iOS can be accessed only through enterprise store. Content on Android, and Windows can be downloaded to the device.

Mobile Content Management consists of the following stages.

- **Content definition:** Administrators upload the content to the EMM console and organize the content in folders.
- **Target Definition:** Administrators target or share their content with users and or groups to make the content available on devices of targeted users.
- **Policy Assignment:** Administrators assign content policies to targets to ensure secure usage of the content. Policies are assigned to folders but apply to each of the files within the folders. For each target, priorities are assigned to policies to ensure that there is no conflict among various policies. The policy with highest priority is resolved against a user. The resolved or applied policy governs the usage of the files, it does not change the content. Priority with lowest value is

considered as highest priority. For example, priority value zero is considered as higher priority than any value equal to or more than one.

- **Distribution:** Based on target definition and policy assignment, folders are made available, or restricted or mandated to users. This is an automated process.

11.1 Files Overview

Files are content that is uploaded, targeted, and distributed among groups or users. The following rules apply to the files system:

- A file can be part of only one folder. If a file is copied into another folder, the copied file will be treated as a separate file.
- The Files list page shows all files as part of the system, and a user can search for these files. Within folders, all files and folders are shown in a hierarchical view. On a server, multiple files with same name and format in a given folder cannot exist. If multiple files of the same format are put in a folder, the files will be automatically renamed as filename(1), filename(2), and so on. Numbering is based on the order in which the files are uploaded, copied, or moved.
- Every time a file is updated, a new version of the file is created. By default, the latest version of the file is shown. You can perform the following actions for previous versions of files.
 - Download - an administrator can access older versions of files.
 - Make as latest version - an administrator can designate an older version rendition of a file as the latest version. The older version is copied into a new version. The file details page displays details of the file versions.
- Supported file types include documents, spreadsheets, presentations, images, audio and video files.
 - PDF, RTF, TXT, XML, DOC, DOCX, XLS, XLSX, CSV, ODP, BMP, GIF, JPEG, JPG, PNG, MP4, MOV, AVI, MP3, PPT and PPTX.

11.2 Files User Interface

The Files screen contains the following user interface elements:

- **+ Add File(s)**: Add a file or several files.
- **File Name**: Displays the name of the file.
 - **Search Files**: Search for files by the name of the file.

- **Format:** Displays the format of the file.
 - **All:** Search for files based on their specific format. This list contains all allowed file formats.
- **Path:** Displays the location of the file .
 - **Search Path:** If you know the file's path, you can search for the path using this feature.
- **Version:** Displays the version number of the file.
 - **Search Version:** Using this feature, you can search for any specific version of the file.
- **Uploaded By:** Displays the user who uploaded the file.
 - **Uploaded By:** If you know the user who uploaded the file, you can search for the file using this feature.
- **Uploaded Date:** Displays file uploaded date and time.
 - **All:** Search for a file based on when it was uploaded. Options range from Today to More than 30 days.
- **Actions:** A list of actions you can take on the file.
 - **Select Action:** Options are Copy To, Move To, and Update.
- **Delete:** Delete files.
- **Previous:** Clicking this button takes you to the previous page (if it exists).
- **Next:** Clicking this button takes you to the next page (if it exists).

Files

[+ Add File\(s\)](#)

Displaying 1 - 1 of 1 - Display

| <input type="checkbox"/> | File Name | Format | Path | Version | Uploaded By | Uploaded Date | Actions |
|---|--|--|---|--|-------------|---|---|
| <input type="text" value="Search Files"/> | All | <input type="text" value="Search Path"/> | <input type="text" value="Search Ver"/> | <input type="text" value="Uploaded By"/> | All | | |
| <input type="checkbox"/> |  CustomMetrics(PDF) | pdf | / | 1.001 | admin | 01 Dec, 2014 23:00:31 EST | <input type="text" value="Select Action"/> |
| <input type="button" value="Delete"/> | | | | | | <input type="button" value="Previous"/> | <input type="button" value="Page {1/1}"/> <input type="button" value="Next"/> |

11.2.1 File Details Page

The File details page contains three tabs by default. In case the file has more than one version, a fourth tab, a Past Version tab is available.

CustomMetrics(PDF)
Format: pdf
Current Version: 1.001

Update Rename
Copy Move
Delete

Description Current Version

File Name CustomMetrics(PDF)
Path /
Description Enter Description

Save & Exit Save & Continue Cancel

- **Description tab:** The description tab displays details of the file, the path it is in, and a brief description about the file by the user who uploaded the file.
- **Current Version tab:** The current version tab displays the version of the file, name of the user who updated it, and the date that the document was last updated. Click the download button to download the current version to your computer.
- **Past Version tab:** The past version tab displays past versions of the file, the name of the user who updated the file, and the date that the document was last updated. Click the download button to download the file's current version to your computer. Click the make current button to turn the specific version of a file you are viewing into the current version.

- **Save & Exit:** This feature allows you to save modifications you made on the **Files Details** page and exit to the Files page.
- **Save & Continue:** The save & continue feature allows you to save changes you made on the Files Details page and remain on the same page.
- **Cancel:** The Cancel button allows you to cancel all changes you made in the Files Details page.

11.3 Applying Actions to Files

You can manage your files through several functions in the content management section of the management console. This section will show you how to add a new file, update a file, rename a file, copy a file, move a file, delete a file, change a file's description, and work with current and previous versions of a file.

11.3.1 How to Add a New File

To add a new file, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Files**. The Files page appears.
2. Click **Add File(s)**. The Add File(s) dialog appears.
3. Select file(s). Click to add, or drag and drop.
4. **Click Add**. The Open Dialog appears.
5. Navigate to the file you want to upload, and select the file. Or Drag and drop the file you want to add.
6. Click **Upload**. Upload page appears.
7. In the **Description** text box, enter description of the document.
8. From the **Move to Folder**, click the drop down list. The Select Folder text box appears.

Note: Selecting a folder is optional. If you do not select a folder, the file is created in the root folder.

9. Enter the name of the folder where you want to save the file. Details of the folder appear.
10. Click on the folder to select it.
11. Click **Save**. The new file is uploaded to the system in the selected folder.

Add File(s) x

Supported Formats ⓘ

Select File(s)*

Click add or Drag & Drop here

Description

Enter Description

Move to Folder

11.3.2 How to Update a File

To update a file, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Files**. The Files page appears.
2. Click on a file. The File details page appears.

3. Click **Update**. The Update File window appears.
4. From Update File, click **+Add**. The Open window appears.
5. Navigate to the file you want to upload, and click on the file.

Note: You can only update a file with a file of the same format and name. If you upload a file with a different name, you will be prompted to change the name to that of the existing file. If you decline, the update fails.

6. Click **Save**. A success message appears.
7. Click **OK**.

11.3.3 How to Rename a File

To rename a file, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Files**. The Files page appears.
2. Click on a file. The File details page appears.
3. Click **Rename**. The Rename File window appears.
4. In **New File Name** text box, enter the new name for the file and then click **Rename**.
5. Click **Save**. A success message appears.
6. Click **OK**.

11.3.4 How to Copy a File

To copy a file, follow these steps:

1. In the EMM Management console, under **Content Management**, click **Files**. The Files page appears.
2. Click on a file. The File Details page appears.
3. Click **Copy**. The Copy File window appears.
4. In the **Copy File** text box, enter the name of the folder where you want to copy the file.
5. The folder name appears. Click to select the folder.
6. Click **Copy**. A success message appears.

Note: If a file with the same name and format exists in the target folder, then the copied file will be renamed with the suffix (1).

7. Click **OK**.

11.3.5 How to Move a File

To move a file, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Files**. The Files page appears.
2. Click on a file. The File Details page appears.
3. Click **Move**. The Move File window appears.
4. In Move File text box, enter the name of the folder where you want to move the file.
5. Folder name appears. Click to select the folder.
6. Click **Move**. A success message appears.

Note: If a file with the same name and format exists in the target folder then the moved file will be renamed with the suffix (1).

7. Click **OK**.

11.3.6 How to Delete a File

To delete a file, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Files**. The Files page appears.
2. Select the file you want to delete in the Files page.
3. Click **Delete** at the bottom of the list of files to delete the file. A confirmation message appears.
4. Click **Yes** to delete the file. A success message appears.

Note: If the file is currently shared or targeted, a user needs to confirm the removal of the current file from sharing and targeting.

5. Click **OK**.
6. Click on a file in the Files Details page. The File Details page appears.
7. Click **Delete**. A confirmation message appears.
8. Click **Yes** to delete the file. A success message appears.

Note: If the file is currently shared or targeted, user needs to confirm removal of current file from sharing and targeting.

9. Click **OK**.

Note: Deleting a file will delete all versions of the file.

11.3.7 How to Change the Description of a File

To change the description of a file, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Files**. The Files page appears.
2. Click on a file. The File Details page appears.
3. In the description tab, change the description in the **Description** text box.
4. Click **Save & Exit**.

11.3.8 How to Download a Current Version

To download a current version of a file, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Files**. The Files page appears.
2. Click on a file. The File Details page appears.
3. Click the **Current Version** tab. Details of the current version appear.
4. In the **Current Version** tab, click **Download**. The file downloads.

11.3.9 How to Download a Previous Version

To download a previous version of a file, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Files**. The Files page appears.
2. Click on a file. The File Details page appears.

3. Click the **Previous Version** tab. Details of the previous version appear.
4. In the **Past Version** tab, click **Version** text box. A search box opens.
5. Enter the version of the document you want to view in the search box. A list of available versions appears.
6. Click the version you want to download. The Download button is activated.
7. Click **Download**. The file downloads.

11.3.10 How to Designate a Previous Version as Current

To designate a previous version of a file as current version, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Files**. The Files page appears.
2. Click on a file. The File Details page appears.
3. Click the **Previous Version** tab. Details of the previous version appear.
4. In the **Past Version** tab, click the Version text box to open it.
5. Enter the version of the document you want to view in the search box. A List of available versions appears.
6. Click the version you want to make current. The Make Current button is activated.
7. Click **Make Current**. The Make Current window appears.
8. Click **Yes**. A success message appears.
9. Click **OK**.

Note: Note that the version number is incremental. For example, the file has three versions . You designate the second version as current. The new version will be No. 4.

11.4 Folders Overview

Folders are entities that contain files and / or other folders. Administrators can target content to users through folders. Enterprise space files cannot be targeted to users directly. If a file is not part of a folder, it cannot be targeted to any user or group.

If a file or folder is added to a folder, it inherits the targeting and policies from the parent folder. The targeting cannot be overwritten but only added to. Policies applied to targets can be overwritten in the child folder, if the administrator applies different policies for the same target.

If folder A is inside folder B, then the targeting of folder A stands for the contents of folder A and also policies applied on the folder. Targeting and policies assigned to folder B do not apply to contents of folder A. If folder A has no targeting and policies, it inherits targeting and policies from folder B.

The following can be done with/to Folders:

- Adding new files or folders
- Removing files or folders
- Adding/Removing targeting including policies
- Deleting folders

11.5 Folders User Interface

The user interface page for folders contains three tabs.

- **Enterprise Space** : Displays content uploaded by the administrator with the intent of distributing it to members of an organization. Policies can be applied to this content per target.
- **User Space**: Displays content uploaded by a user. An administrator can define the policy that governs all content for a user's space. Policies applicable are not at the folder level but for all content for a user.
- **Shared Space**: Displays content shared by all users with other users.

11.5.1 Folders Page

The Folders page contains details of various folders that are available for a user. Users can create folders and organize content in these folders. Based on who creates the content, folders are categorized under Enterprise Space, User Space and Shared Space.

Folders

| Enterprise Space | User Space | Shared Space | | |
|--|--|--|---|--|
| <input type="button" value="+ New Folder"/> Displaying 1 - 2 of 2 - Display <input type="text" value="10"/> | | | | |
| Folders Name | Path | Last Modified By | Last Modified On | Action |
| <input type="text" value="Search Folders"/> | <input type="text" value="Search Path"/> | <input type="text" value="Search Last Modified By"/> | <input type="text" value="All"/> | |
| <input type="checkbox"/> Luke | /Anakin | admin | 01 Dec, 2014 23:56:55 EST | <input type="button" value="Select Action"/> |
| <input type="checkbox"/> Anakin | / | admin | 01 Dec, 2014 23:56:44 EST | <input type="button" value="Select Action"/> |
| <input type="button" value="Delete"/> | | | <input type="button" value="Previous"/> Page {1/1} <input type="button" value="Next"/> | |

- **Enterprise Space:** Displays details of folders created by an administrator.
 - **New Folder:** Using this button, you can add a folder.
 - **Folders Name:** Displays the name of a folder.
 - **Search Folders:** Search for a folder by its name.
 - **Repository:** Displays the folder repository details. Possible options are Local or a SharePoint path.
 - **Path:** Displays the location of the folder.
 - **Search Path:** If you know the path of a folder, you can search for the folder using the path.
 - **Last Modified By:** Displays the name of the user who last modified the folder.
 - **Search Last Modified By:** Search for the folder using the name of the last user who modified the folder.

- **Last Modified On:** Displays date and time folder was last modified.
 - **All:** Search for a folder based on when it was last modified. Available options range from Today to Last 30 days.
- **Action:** Provides you with a list of actions you can take on a folder.
 - **Select Action:** Available options are Copy To and Move To.
- **Delete:** Use this button to delete a folder.
- **Previous:** Click this button to navigate to the previous page.
- **Next:** Click this button to navigate to the next page.

11.5.2 Enterprise Space

The Enterprise Space is meant for the enterprise to provide and distribute content to users and groups. Content in this space is controlled by administrators. Administrators can target folders and apply policies to folders per target.

Enterprise Space

Enterprise Space > Luke

/Anakin/Luke



Luke

Last Modified By: admin

Last Modified On: 01 Dec, 2014 23:56:55 EST

| | |
|-------------|---------------|
| Copy To | Move To |
| Copy From | Move From |
| Add File(s) | Create Folder |
| Rename | Delete |

Details

Content

Targeting

Folder Name Luke

Path /Anakin

Description

Enter Description

Save & Exit

Save & Continue

Cancel

For Enterprise Space folders, a user can perform the following actions.

Important: The following actions are not applicable to SharePoint repository folders.

- **Copy to** - A user can copy a folder to a destination a user specifies. All internal files and folders of the folder are also copied to the new destination. If a folder with same name exists in the destination folder, the new folder will be renamed with a suffix (1). The latest version of the file is copied.

- **Move to** - A user can move a folder to a destination a user specifies All internal files and folders of the folder are also moved to the new destination. If a folder with same name exists in the destination folder, the new folder will be renamed with a suffix (1). All versions of the file are moved.
- **Copy From** - The files or folders from the source location are copied to current folder. All sub folders and files are also copied. If a folder with the same folder name is present in the destination, the new folder will be renamed with a suffix (1). The latest version of the file is copied.
- **Move From** - The files or folders from the source location are moved to current folder. All sub folders and files are also moved. If a folder with the same folder name is in the destination, the new folder will be renamed with a suffix (1). All versions of the file are moved.
- **Add Files** - A new file or multiple files can be added to the current folder.
- **Create Folder** - A new folder can be created within the current folder.
- **Rename** - The folder can be renamed. If a folder with the same folder name is already present in the destination, the new folder will be renamed with a suffix (1).
- **Delete** - When a folder is deleted, it is removed from all locations including the device. If a folder is currently targeted, a user must confirm the removal of existing targets on the folder.

11.5.2.1 Details Tab

The Details tab displays details about the folder:

- **Folder Name:** Displays the name of the folder.
- **Path:** Displays the location of the folder.
- **URL:** The SharePoint folder URL. This field is not visible for local folder.
- **Description:** Displays a brief description of the folder as entered by the administrator.

The screenshot shows a web interface with three tabs: 'Details', 'Content', and 'Targeting'. The 'Content' tab is selected. Below the tabs, there are three fields: 'Folder Name' with the value 'Luke', 'Path' with the value '/Anakin', and 'Description' with a text input area containing the placeholder 'Enter Description'.



11.5.2.2 Content Tab

The Content tab displays various files and folders within the folder:

Important: The Content tab is available only for local folders. This tab is not available in the details page of a repository/SharePoint folder.

- **File/Folder Name:** Displays the name of the file/ folder.
 - **Search Files/Folders:** You can search for files/folders by the name of the file/folder.
- **Format:** Displays the format of the files.
 - **All:** Search for files based on their specific format. The list contains all allowed file formats.
- **Path:** Displays the location of the file/folder.
 - **Search Path:** If you know the path of a file/folder, you can search for the file/folder using this feature.
- **Last Modified By:** Displays the name of the user who last modified the file/folder.
 - **Search Last Modified By:** Search for a file/folder using the name of the last user who modified the file/folder.

- **Last Modified Date:** Displays the date and time a file/folder was last modified.
 - **All:** You can search for a file/folder based on when it was last modified. Options range from Today to Last 30 days.
- **Action:** A list of actions you can take on the file/folder.
 - **Select Action:** Options are Copy To and Move To.
- **Delete:** Use this button to delete a folder.
- **Previous:** Click this button to go to the previous page.
- **Next:** Click this button to go to the next page.

| Details Content Targeting | | | | | | |
|---------------------------|---|--------|--|--|---------------------------|-----------------|
| <input type="checkbox"/> | File / Folder Name | Format | Path | Last Modified By | Last Modified On | Actions |
| | <input type="text" value="Search Files / Folders"/> | All ▾ | <input type="text" value="Search Path"/> | <input type="text" value="Search Last Modified By"/> | All ▾ | |
| <input type="checkbox"/> |  Padme | pdf | /Anakin/Luke | admin | 02 Dec, 2014 00:10:16 EST | Select Action ▾ |
| <input type="checkbox"/> |  Leia | pdf | /Anakin/Luke | admin | 02 Dec, 2014 00:10:16 EST | Select Action ▾ |
| Delete | | | | Previous Page {1/1} Next | | |

11.5.2.3 Targeting Tab

Targeting tab allows an enterprise administrator to target content to users and groups.

- **Add Users:** You can enter user IDs of users in order to share the content.
- **Add Groups:** You can enter names of groups in order to share the content.
- **Target:** Displays details of users and groups targeted for the enterprise content.
- **Policy:** Displays applied policy for the user or a group for targeting.
- **Priority:** Displays the priority applied for targeting for the user or group.

- **Inherited Targeting:** Displays details of targeting inherited by a user or a group from parent folders.
- **Target:** Displays the details of a user or a group who inherited the targeting.
- **Inherited From:** Displays details of a parent folder the user or a group inherited targeting from.
- **Policy:** Displays policies applied for the user or a group.
- **Priority:** Displays the priority applied for targeting for the user or a group.

Details
Content
Targeting *

Add Users

Add Groups

| | Target | Policy | Priority |
|--------------------------|--------|--------|----------------|
| <input type="checkbox"/> | han | None | Not Applicable |
| <input type="checkbox"/> | Jedi | None | Not Applicable |

Inherited Targeting

| Target | Inherited From | Policy | Priority |
|------------------|----------------|--------|----------|
| No results found | | | |

11.5.3 User Space

User space is the space where users upload their content. In the Management Console, the administrator can only view content in this space and cannot modify the files uploaded by a user.

An administrator can prescribe a policy for all content in user space. Each user in EMM has a user space. Users can only upload files and folders to their user spaces. Users can also share files and folders with other users. Shared files and folders are visible in the shared space tab of the recipient users. Users can upload and share content through the self-service portal.

- **User Space Policies:** Using this button, you can assign policies to user spaces.
- **User Space:** Displays user space folder name.
 - **Search User Space:** Search folders using the user space name.
- **Last Modified On:** Displays the date and time the file or folder was last modified.
 - **All:** Search a file or folder based on when it was last modified. Options range from Today to Last 30 days. Search for user spaces based on the last modified date.
- **Previous:** Click this button to go to the previous page.
- **Next:** Click this button to go to the next page.


The screenshot displays the 'User Space' section of the Kony Management Console. At the top, there are three tabs: 'Enterprise Space', 'User Space', and 'Shared Space'. Below the tabs, there is a '+ User Space Policies' button and a display count 'Displaying 1 - 1 of 1 - Display' with a dropdown menu set to '10'. The main content area is a table with two columns: 'User Space' and 'Last Modified On'. The 'User Space' column contains a search box labeled 'Search User Space' and a folder icon labeled 'han'. The 'Last Modified On' column contains a dropdown menu set to 'All' and the date and time '02 Dec, 2014 00:23:54 EST'. At the bottom of the table, there are navigation buttons: 'Previous', 'Page {1/1}', and 'Next'.

11.5.3.1 User Space

When you click on any of the user's folder, the associated user space page appears.

- **Content:** Displays available content details.

han's User Space

| File / Folder Name | Path | Last Modified By | Last Modified On |
|---|--|--|---|
| <input type="text" value="Search Files / Folders"/> | <input type="text" value="Search Path"/> | <input type="text" value="Search Last Modified By"/> | <input type="text" value="All"/> |
|  Allies | / | Han | 02 Dec, 2014 00:23:43 EST |
| | | | <input type="button" value="Previous"/> <input type="button" value="Page {}/"/> <input type="button" value="Next"/> |

- **Policy Details:** Displays applicable policy.

han's User Space

| Content | Policy Details |
|---|----------------|
| User Id han | |
| Policy Applied Empire <input type="button" value="Modify"/> | |
| Policy Inherited From Not Applicable | |

- **Modify:** Use this button to change the policy that is applied on the folder.

You can view policies applied on users by an administrator in the policy details tab. Only an administrator can modify these policies.

11.5.4 Shared Space

The Shared Space tab displays content shared by other users with a current user. Each user has his or her own shared space, and all content shared with each user is available in this tab.

An administrator can assign policies to the shared space, and all constituent files and folders will inherit those policies.

The screenshot displays the 'Shared Space' tab interface. At the top, there are three tabs: 'Enterprise Space', 'User Space', and 'Shared Space'. Below the tabs, there is a '+ Shared Space Policies' button and a 'Displaying 1 - 1 of 1 - Display 10' indicator. The main content area is a table with two columns: 'Shared Space' and 'Last Modified On'. The table contains one row with a folder icon, the name 'obiwan', and the date '02 Dec, 2014 01:30:00 EST'. At the bottom of the table are 'Previous', 'Page {1/1}', and 'Next' buttons.

- **Shared Space Policies:** Using this button, you can create new shared space policies. You can assign policies to user's shared space.
- **Shared Space:** Displays a user's shared space folder name.
 - **Search Shared Space:** You can search for folders using the name of the shared space.
- **Last Modified On:** Displays the date and time the file or folder was last modified.
 - **All:** You can search for a file/folder based on when it was last modified. Options range from Today to Last 30 days.
- **Previous:** Click this button to go to the previous page.
- **Next:** Click this button to go to the next page .

11.6 Applying Actions to Folders

11.6.1 How to Create a New Folder in the Local Repository

To create a new folder, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Folders**. The Folders page appears.
2. Click **Add Folder**. The Add Folder dialog appears.
3. From the Repository list, select the **Local**.
4. In the **Folder Name** text box, enter a name for the folder.
5. In the **Description** text box, enter description about the folder.
6. Click **Create**. A success message appears.
7. Click **OK**. The Folders page appears with the newly created folder in it.
8. Click **Create & Exit**. The Folders page appears.

11.6.2 How to Create a New Folder From a SharePoint Repository

To create a new folder, follow these steps:

1. In EMM Management Console, under **Content Management**, click **Folders**. The Folders page appears.
2. Click **Add Folder**. The Add Folder dialog appears.
3. From the Repository list, select a SharePoint repository. The Repository Root Path field appears.

Note: These SharePoint repositories are created by you or another enterprise administrator.

4. From the **Content Type** list, select the content type. Options are Site, Document Library, and Folder.

The screenshot shows a dialog box titled "Add a Folder" with a close button in the top right corner. The dialog contains the following fields and controls:

- Repository:** A dropdown menu with "Test" selected.
- Repository Root Path:** A text box containing the URL "https://konyone.sharepoint.com/sites/Kony/DevelopmentPlatform/Management/EMM/".
- Content Type*:** A dropdown menu with "Folder" selected.
- Content URL*:** A text box containing the URL "https://konyone.sharepoint.com/sites/Kony/DevelopmentPlatform/Ma".
- Description:** A text area with the placeholder text "Enter Description".

At the bottom of the dialog, there are three buttons: "Create", "Create & Edit", and "Cancel".

5. In the **Content URL** text box, enter the content URL.
6. In the **Description** text box, enter a description about the folder.
7. Click **Create**. A success message appears.
8. Click **Create & Exit**. The Folders page appears.

11.6.3 How to Search Folders

To search for a folder, follow these steps:

1. In the **Enterprise** tab, in **Search Folders** text box, enter part or all of the name of the folder.
2. A list of folders appears, based on the text you entered.

3. Select the folder you want to open.

11.6.4 How to Search for a Path

To search for a path, follow these steps:

1. In the **Enterprise** tab, in **Search Path** text box, enter the name of the path you want to search.
2. A list of folders in paths appears, based on the text you entered.
3. Select the folder in the path that you want to open.

11.6.5 How to Search Using Last modified By

To search for a folder using last modified by feature, follow these steps:

1. In the **Enterprise** tab, in **Search Last Modified by** text box, enter the name of the user who last modified the folder.
2. A list of folders last modified by the specified user appears.
3. Select the folder you want to open.

11.6.6 How to Search Using Last Modified On

To search for a folder using last modified on feature, follow these steps:

1. Under the **Enterprise** tab, from the **Search Last Modified On** drop-down list, select one of the options.
2. A list of folders last modified on the specified date appears.
3. Select the folder you want to open.

11.6.7 How to Manage a User Space Policy

To manage a user space policy, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Folders**. The Folders page appears.
2. Click the **User Space** tab. The User space tab details page appears.
3. Click **User Space Policies**. The User Space Policies dialog appears.
4. In the **Add Users** box, enter the name of the user you want to add the policy on, and click **Add**. Target details appear.
5. In the **Add Groups** box, enter the name of the group you want to add the policy on and click **Add**. Target details appear.
6. From the **Policy** drop-down list, select the policy you want to apply and click **Save**. A success message appears.
7. Click **OK**.

11.6.8 How to Assign a Policy to User's User Space

To assign a policy to user's user space, follow these steps:

1. In the **Add User** text box, enter a user name.
2. Click **Add**.
3. A user is added in the Target section. A confirmation message that the policy is mandatory also appears.
4. In the **Target** section, from the **Policy** drop-down list, select the policy to apply for the user and click **Save**. A success message appears.
5. Click **OK**.

11.6.9 How to Assign a User Space Policy to a Group

To assign a user space policy to a group, follow these steps:

1. In the **Add Group** text box, enter a group name in it.
2. Click **Add**.
3. A group is added in the target section A confirmation message that the policy is mandatory appears.
4. In the **Target** section, from the **Policy** drop-down list, select the policy to apply for the group and click **Save**. A success message appears.
5. Click **OK**.

11.6.10 How to Search User Space

To Search for a user space, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Folders**. The Folders page appears.
2. Click the **User Space** tab. The tab details page appears.
3. Enter the name of the desired user space in the **Search User Space** text box, and press **Enter**. A list of user spaces appear. .
4. Click the user space you want to view. User space details appear.

11.6.11 How to search using Last Modified on

To search for a folder based on last modified on feature, follow these steps:

1. In the **User Space** tab, from the **Last Modified On** list, select when the folder was last modified.

Note: Options include Today, Yesterday, Last 7 days, Last 10 days, and Last 30 days.

2. Select the time period. A list of folders appears, based on the time selected.

11.6.12 How to Manage User Shared Space Policy

To manage a user shared space policy, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Folders**. The Folders page appears.
2. Click the **Shared Space** tab. The Shared space details page appears.
3. Click **Shared Space Policies**. The Shared Space Policies dialog appears.
4. In the **Add Users** box, enter the name of the user you want to add the policy on, and click **Add**. The target details appear.
5. In the **Add Groups** box, enter the name of the group you want to add the policy on, and click **Add**. The target details appear.
6. From the **Policy** drop-down list, select the policy you want to apply, and click **Save**. A success message appears.
7. Click **OK**.

11.6.13 How to Assign a Policy to a User's Shared Space

To assign policy to a user's shared space, follow these steps:

1. In the **Add User** text box, enter a user name.
2. Click **Add**.
3. A user is added in the Target section. A message **Policy is Mandatory** displays.
4. In the Target section, from the **Policy** drop-down list, select the policy to apply for the user, and click **Save**. A success message appears.
5. Click **OK**.

11.6.14 How to Assign a Shared Space Policy to a Group

To assign a shared space policy to a group, follow these steps:

1. In the **Add Group** text box, enter a group name.
2. Click **Add**.
3. The group is added in the target section. The message **Policy is Mandatory** displays.
4. In the Target section, from the **Policy** drop-down list, select the policy to apply for the group, and click **Save**. A success message appears.
5. Click **OK**. User space tab details appear.

11.6.15 How to Search a Shared Space

To Search for a shared space, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Folders**. The Folders page appears.
2. Click the **Shared Space** tab. The details page for the Shared Space tab appears.
3. Enter the name of the desired shared space in the **Search Shared Space** text box, and press **Enter**. Results appear.
4. Click the **Shared Space** you want to view. Shared space details appear.

11.6.16 How to Search Using Last Modified On

To search for a shared space based on last modified on feature, follow these steps:

1. In the **Shared Space** tab, from the **Last Modified On** list, select when the folder was last modified.

Note: Options include Today, Yesterday, Last seven days, Last 10 days, and Last 30 days.

All folders modified in the time period you have selected appears.

11.6.17 How to Copy a Folder to Another Folder

To copy a folder to another folder, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Folders**. The Folders page appears.
2. Click on any folder. The Enterprise space page appears.
3. Click **Copy To**. The Copy Folder window appears.
4. In the Destination Folder text box, enter the name of the folder you are copying to.
5. Click the folder name to select the folder and then click **Copy**.
6. A **Copy to Successful** message appears. Click **OK**.

11.6.18 How to Move a Folder to Another Folder

To move a folder to another folder, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Folders**. The Folders page appears.
2. Click on any folder. The Enterprise space page appears.
3. Click **Move To**. The Move Folder window appears.
4. In the **Destination Folder** text box, enter the name of the folder where the other folder will be moved. Folder name appears.
5. Click the folder name to select the folder, and then click **Move**.
6. A **Move to Successful** message appears. Click **OK**.

11.6.19 How to Copy From a Folder

To copy a folder from another folder, follow these steps:

1. In the EMM Management console, under **Content Management**, click **Folders**. The Folders page appears.
2. Click on any folder. The Enterprise space page appears.
3. Click **Copy From**. The Copy From window appears.
4. In the **Source Folder(s)** text box, enter the name of the folder you want to copy from.
5. Click the folder name to select the folder.
6. In the Source File(s) text box, enter the name of the file you want to copy. File name appears.
7. Click the file name to select the file and then click **Copy**.
8. A **Copy From Successful** message appears. Click **OK**.

11.6.20 How to Move a Folder

To move a folder from one location to another, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Folders**. The Folders page appears.
2. Click on any folder. The Enterprise space page appears.
3. Click **Move From**. The Move From window appears.
4. In the **Source Folder(s)** text box, enter the name of the folder you want to move from. Folder name appears.
5. Click the folder name to select the folder.
6. In the **Source File(s)** text box, enter the name of the file you want to move. File name appears.

7. Click the file name to select the file and then click **Move**.
8. A **Move From Successful** message appears. Click **OK**.

11.6.21 How To Add Files

To add files to a folder, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Folders**. The Folders page appears.
2. Click on any folder. The Enterprise space page appears.
3. Click **Add File(s)**. The Add File(s) dialog appears.
4. Select file(s). You can do this in two ways. Click to add or Drag and drop.
5. Click **+ Add**. The Open dialog appears.
6. Navigate to the file you want to upload, and select the file. Or Drag and drop the file you want to add.
7. Click **Upload**.
8. In the **Description** text box, enter a brief description about the document.
9. Enter the name of the folder where you want to save the file. Details of the folder display.
10. Click on the folder to select it.
11. Click **Save**. The new file is uploaded to the system in the folder you have specified.

11.6.22 How To Create a Folder

To create a new folder, follow these steps:

1. In the EMM Management console, under **Content Management**, click **Folders**. The Folders page appears.
2. Click on any folder. The Enterprise space page appears.
3. Click **Add Folder**. The Add Folder dialog appears.
4. In the **Folder Name** text box, enter a name for the folder.
5. In the **Description** text box, enter a description about the folder.
6. Click **Create**. A success message appears.
7. Click **OK**. The Folders page appears with the newly created folder in it.

11.6.23 How To Rename a Folder

To rename a folder, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Folders**. The Folders page appears.
2. Click on any folder. The Enterprise space page appears.
3. Click on a folder. The Folder details page appears.
4. Click **Rename**. The Rename Folder window appears.
5. In **New Folder Name** text box, enter the new name for the folder, and then click **Rename**.
6. Click **Save**. A success message appears.
7. Click **OK**.

11.6.24 How to Delete a Folder

To delete a folder, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Folders**. The Folders page appears.
2. Click on any folder. The Enterprise space page appears.
3. Click on a folder. The Folder details page appears.
4. Click **Delete**. The Delete Folder Confirmation window appears.
5. Click **OK** to delete the folder. A success message appears.
6. Click **OK**.

11.6.25 How to Add Users for Targeting

To add a user for targeting folders, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Folders**. The Folders page appears.
2. Click on any folder. The Enterprise space page appears.
3. Click on Targeting tab. The Targeting tab details appear.
4. Enter the name of the user in the **Add User** text box and click **Add**. The user is added, and details display in the target section.
5. From the **Policy** list, select the policy you want to apply to the user.
6. Click **Save & Continue**. A success message appears.
7. Click **OK**.

Important: Availability of content on your devices is strictly based on content policy applied.

11.6.26 How to Add Groups for Targeting

To add a group for targeting a folder, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Folders**. The Folders page appears.
2. Click on any folder. The Enterprise space page appears.
3. Click on Targeting tab. The Targeting tab details appear.
4. Enter the name of the group in the **Add Group** text box, and click **Add**.
5. The group is added, and details display in the target section .
6. From the **Policy** list, select the policy you want to apply to the group.
7. In the **Priority** text box, enter the priority you want to assign to the policy.
8. Click **Save & Continue**. A success message appears.
9. Click **OK**.

Important: Availability of content on your devices is strictly based on content policy applied.

11.7 Content Policies

Content policies are used in the targeting process of folders. While defining access rights to each of the users or groups, content policies are applied to define the use of the content files.

Content policies are defined to control the use of content files on devices. This ensures appropriate access, data security, and avoid abuse.

Policies are applied to folders to govern each file that is part of a folder and are applicable only to the specified user or group.

The following actions are possible on the Content Policy list page:

- Filtering
- Modifying state
- Modifying status
- Copying the Policy - The administrator can copy a policy. However, the administrator must provide a new name for the policy. The administrator can then modify the policy as required.
- Accessing policy details
- Deleting the policy

Content Policy details page has four tabs.

- Policy Basics
- iOS
- Android
- Windows

11.7.1 Policy Basics

- **Policy Name:** Displays the name of the policy.
- **Description:** Displays the description of the policy as entered by the user. You can modify this.

11.7.2 iOS

The iOS tab provides various content usage rules and content availability policies. You can select from the options available on how to share the content through iOS devices.

Important: Users can share content based on policies specified in this section.

Content Usage Rules

For Content Usage Rules, you can choose from Yes or No on how the content can be shared.

Note: If a file is open when the policy is applied, content policy will not reflect on it. Policies are applied once the file is closed and then re-opened.

By default most of the fields below are set to **Yes**.

- **Allow Post To Facebook**
- **Allow Post To Twitter**
- **Allow Message.** This feature not yet available for iPad Mini/iOS8.1
- **Allow Mail**
- **Allow Print**
- **Allow Copy To Pasteboard**
- **Allow Assign To Contact**
- **Allow Save To Camera Roll**

- **Allow Add To Reading List**
- **Allow AirDrop**
- **Configure Expiration:** By default this is set to **None**. You can change this to **Date**. When you select date, Expiration Date text box appears.
 - **Expiration Date** (Text box): Select the date from the calendar chooser.

You can also make the content available based on geographical location and time. To set a Geofence rule, select the geofence rule you want to apply from the list of rules available. To set time fence rule, select the time fence rule you want to apply from the list of rules available.

- **Geofence Rule:** You can enter the geofence rule you want to apply on the content.
- **Time Fence Rule:** You can enter the time fence rule you want to apply on the content.

11.7.3 Android

- **Allow Access in Android:** By default, this is set to **Yes**.

11.7.4 Windows

- **Allow Access in Windows:** By default, this is set to **Yes**.

11.8 Applying Content Policies

11.8.1 How to Create a New Content Policy

To create a new content policy, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Content Policies**. The Content Policies page appears.
2. Click **New Content Policy**. The New Content Policy page appears.
3. In the **Policy Name** text box, enter policy name.

4. In the **Description** text box, enter a description for the policy.
5. Click **Create & Exit**. A success message appears.
6. Click **OK**. The Content Policy page appears. The policy is in draft status.
7. From the **State** dropdown list, select **Active**. The Content Policy State Change window appears.
8. In the **Comments** text box, enter routing comments and click **Change State**. A success message appears.
9. Click **OK**.
10. To change the state to draft, in the **State** dropdown list, select **draft**. The Content Policy State Change window appears.
11. In the **Comments** text box, enter routing comments and click **Change State**. A success message appears.
12. Click **OK**.
13. In the **Status** drop-down list, select **Publish**. The Content Policy Status Change window appears.
14. In the **Comments** text box, enter comments, and click **Publish**. A success message appears.
15. Click **OK**.
16. If you want to unpublish this policy, from the **Status** list, select **Unpublish**. The Content Policy Status Change window appears.
17. In the **Comments** text box, enter comments, and click **Unpublish**. A success message appears.
18. Click **OK**.

11.8.2 How to Search for a Content Policy

To search for a content policy, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Content Policies**. The Content Policies page appears.
2. In the **Search Policies** text box, enter the name of the specified policy.
3. A list of policies that contain the details you entered appears.
4. Select the policy you want to open.

11.8.3 How to Search for a Policy From the State drop-down list

To search for a policy from the State drop-down list, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Content Policies**. The Content Policies page appears.
2. Under the State column, click **All States** drop-down list. The **Draft** and **Active** states appear.
3. Select the state. The page refreshes and displays all policies in that state.
4. Select the policy you want to open.

11.8.4 How to Search for a Policy From the Status drop-down list

To search for a policy from the status drop-down list, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Content Policies**. The Content Policies page appears.
2. Under the Status column, click the **All Statuses** drop-down list. The **Published** and **Unpublished** statuses appear.
3. Select the status. The page refreshes and displays all policies in that status.
4. Select the policy you want to open.

11.8.5 How to Search for a Policy From Search Modified By

To search for a policy based on when it was last modified, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Content Policies**. The Content Policies page appears.
2. In the **Search modified by** text box, enter the name of the user. A list of policies modified by the user appears.
3. Select the policy you want to open.

11.8.6 How to Search for a Policy by Last Modified On

To search for a policy based on when it was last published, follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Content Policies**. The Content Policies page appears.
2. From the **Search Last modified On** drop-down list, select the time period. A list of policies modified in that time period appears.
3. Select the policy you want to open.

11.8.7 How to Search for a Policy from Last Published On

To search for a policy by blast published on feature, follow these steps:

1. In the EMM Management console, under **Content Management**, click **Content Policies**. The Content Policies page appears.
2. From the **Search Last Published On** drop-down list, select the time period. A list of policies published in that time period appears.
3. Select the policy you want to open.

11.8.8 How to Use the Actions Button

Using the Actions feature, you can copy a policy. Follow these steps:

1. In the EMM Management Console, under **Content Management**, click **Content Policies**. The Content Policies page appears.
2. Search for the policy you want to copy. Policy details appear.
3. From the **Select Action** drop-down select **Copy Policy**. The Copy Content Policy page appears.
4. Enter new policy name and click **Copy**. A success message appears.
5. Click **OK**.

11.9 Content Repositories

In the Content Management section, before Kony Management Suite 3.5, Enterprise content is uploaded only by an administrator. To extend the enterprise content feature to include files and folders from the enterprise SharePoint, a new Repositories feature is introduced in Kony Management Suite 3.5 GA. The Repositories feature in the Content Management section of Kony Management Suite enables an administrator to connect the content section of the enterprise store on a device to the Microsoft SharePoint environment. The Sharepoint administrator determines whether an end user can access files and folders. The Repositories feature helps an administrator:

- Add a new SharePoint repository.
- Add folders from SharePoint to appear on a device with all folder contents.

11.9.1 Repositories

The rRepositories page displays the available repositories in Kony Management Suite. You can also create a new repository in this page.

The Repositories screen appears with the list of repositories. The list view displays a list of all repositories along with other details. You can search the repositories based on each column.

The Repositories list view displays the following columns:

| Column | Description |
|------------------|---|
| Repository Name | Displays the repository name. |
| Type | Displays the repository type. Three types of repositories are supported: <ul style="list-style-type: none"> SharePoint Server 2010 SharePoint Server 2013 SharePoint Online 2013 |
| Server URL | Displays the server URL. |
| Last Modified By | Displays the user who last modified the repository details. |
| Delete | Selected repositories can be deleted. This button is only active if the check box next to Repository Name is selected or if the multi-select check box is selected. |

You can navigate the list view using the **Previous** and the **Next** buttons.

You can do the following from the Repositories page:

- Add a new repository
- Update a repository
- Search for a repository
- Delete a repository

11.9.2 Create a New Repository

To create a new repository, follow these steps:

1. In Kony Management Suite, click **Repositories** under Content Management. The Repositories page appears.
2. Click **New Repository**. The Create Repository page appears.

Create Repository x

Repository Name*

Description

Server URL*

Repository Type*

Authentication Type*

Allow Storing User Credentials On Device

Test Connection Yes No

3. Enter details for the following fields:
 - a. **Repository Name:** Enter a repository name of your choice.
 - b. **Description:** Enter a brief description about the repository.
 - c. **Server URL:** Enter the SharePoint server URL.
 - d. **Repository Type:** Select the repository type. Options are SharePoint Server 2010, SharePoint Server 2013, and SharePoint Online 2013.
 - e. **Site Relative Path:** Enter the site relative path.
 - f. **Authentication Type:** Select the authentication type. Options are Basic, Digest, and NTLM (NT LAN Manager).
 - g. **Use JCIFS Engine:** Select this if you want to use JCIFS engine (available only for the NTLM authentication type). JCIFS is an Open Source client library that implements the Common Internet File System and Server Message Block networking protocol in Java.
 - h. **Allow Storing User Credentials on Device:** Select this option if you want to allow storing credentials on the device.
 - i. **Test Connection:** Select this option if the connection needs to be tested. Options are Yes and No. If you select **Yes**, the following options are enabled:
 - j. **Domain:** Enter the SharePoint domain name.
 - k. **User Name:** Enter your user name details.
 - l. **Password:** Enter the password corresponding to the user name entered earlier.
4. Click **Save**. A confirmation page appears.
5. Click **Yes**. A confirmation page appears.
6. Click **OK**. A new content repository is created.

11.9.3 Update a Repository

To update a repository, follow these steps:

1. In Kony Management Suite, click **Repositories** under Content Management. The Repositories page appears.
2. Click the repository you want to update. The Repository page details appear.
3. Make the required changes and then click **Save**. A confirmation page appears.
4. Click **Yes**. A confirmation page appears.
5. Click **OK**.

11.9.4 Delete a Repository

To delete a repository, follow these steps:

1. In Kony Management Suite, click **Repositories** under Content Management. The Repositories page appears with all existing repositories.
2. Select the repository you want to delete. The Delete button is activated.
3. Click **Delete**. A confirmation page appears.
4. Click **Yes**. A success message appears.
5. Click **OK**. The repository is deleted.

12. Self Service Console

Self Service Console includes following sections:

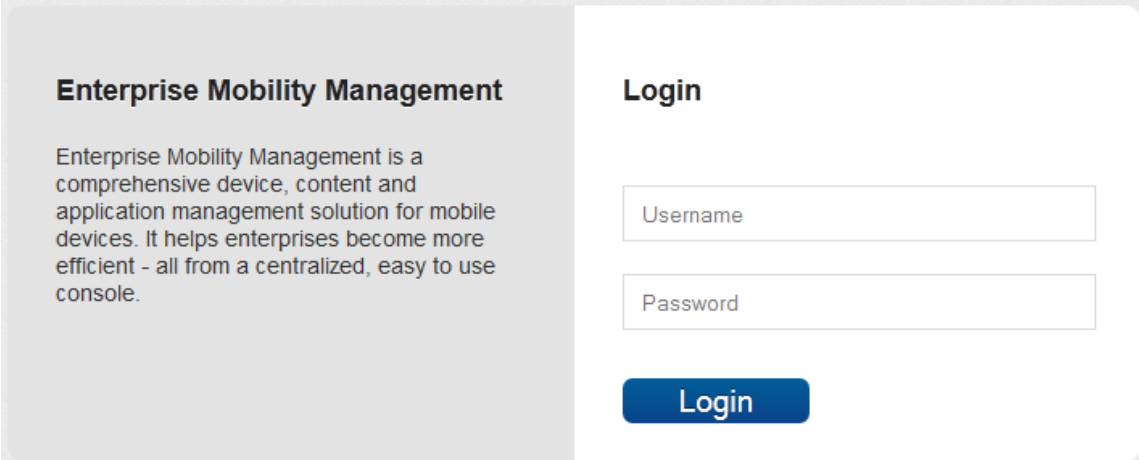
- [Home](#)
- [Devices](#)
- [Content](#)

Note: While both the Admin and the Self Service Console sessions are open in a browser, if a user logs out from any of the Console, results in closing both the active sessions.

12.1 Login

The Kony EMM Console authentication window allows its users to log in to the system. The users with appropriate privileges can log in to EMM Console and perform various operations.

To log in to Self Service console, follow these steps:



Enterprise Mobility Management

Enterprise Mobility Management is a comprehensive device, content and application management solution for mobile devices. It helps enterprises become more efficient - all from a centralized, easy to use console.

Login

Username

Password

Login

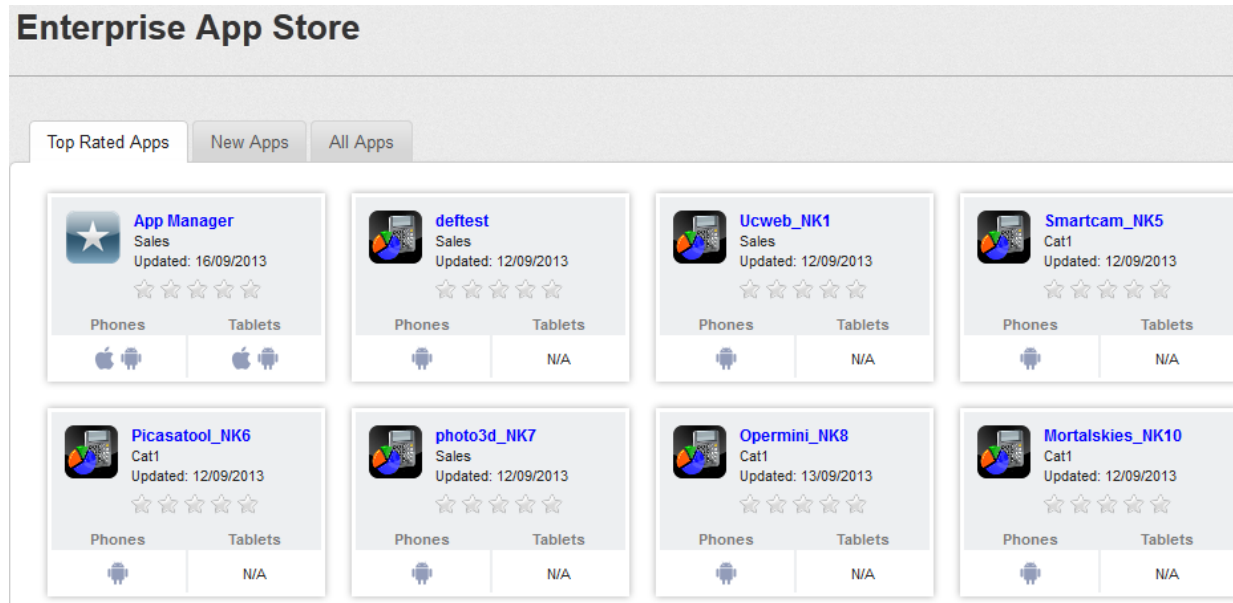
1. Open an Internet browser.
2. Enter the EMM URL in the Address field of the browser. The EMM Console Login screen appears.
3. **User Name:** Enter the user name in the **User name** text field.
4. **Password:** Enter the password in the **Password** text field.
5. Click the **Login** button. After successful authentication, the **Dashboard** screen appears.

If the same user is logged into both the Admin and the Self Service Consoles and the user logs out from any of the consoles, this results in closing both the active sessions. It may require the user to log in into either Console again if they wish to access it.

Note: It is recommended that the same user should not login from multiple browsers or computers. Modifying the same page simultaneously may result into an unexpected behavior.

12.2 Home

By default, **Enterprise App Store page** is the first page you visit after login under **Home** section. An enterprise app store is the place where you should go to find apps details. You can rate and also provide feedback comment for the app that you have downloaded on your device.



The Enterprise App Store page appears with three tabs.

- [Top Rated Apps](#)
- [New Apps](#)
- [All Apps](#)

By default, Top Rated Apps tab is set to active.

12.2.1 Top Rated Apps

This page displays the top rated apps based on overall user rating and comments.

You can perform the following activities from the **Top rated Apps** page:

Enterprise App Store



Javaconnector

Category: General

Created By: akram ali

★☆☆☆☆ (1)

iPad 2.0.0.1

Android Tablet 2.0.0

Downloads 1

Description

Rating ★☆☆☆☆ (0)

Rate & Comment

No Comments found

View More Comments

- Rate and Comment your App

To rate and comment your app, follow these steps:

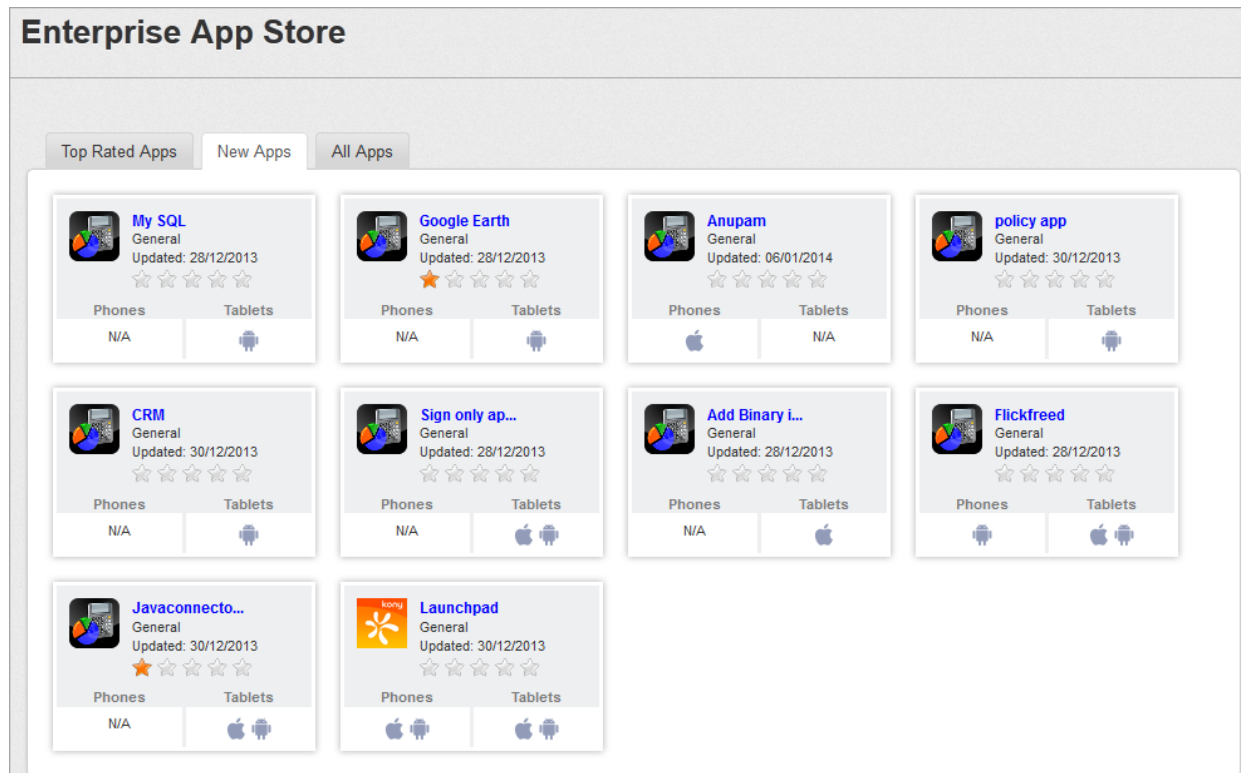
1. **Description:** Enter the comments in the Description text box.
2. **Rating:** Select the number of star icons to rate the app.
3. Click the **Rate and Comment** button to save the details.

The added comment appears in the list. The recent comment becomes the foremost comment in the list.

Click the **View More Comments** button to view other review comments posted by other users.

12.2.2 New Apps

The New Apps page displays all the newly added apps into Enterprise App Store.



You can perform the following activities from the New Apps page:

- Rate and Comment your App

To rate and comment your app, follow these steps:

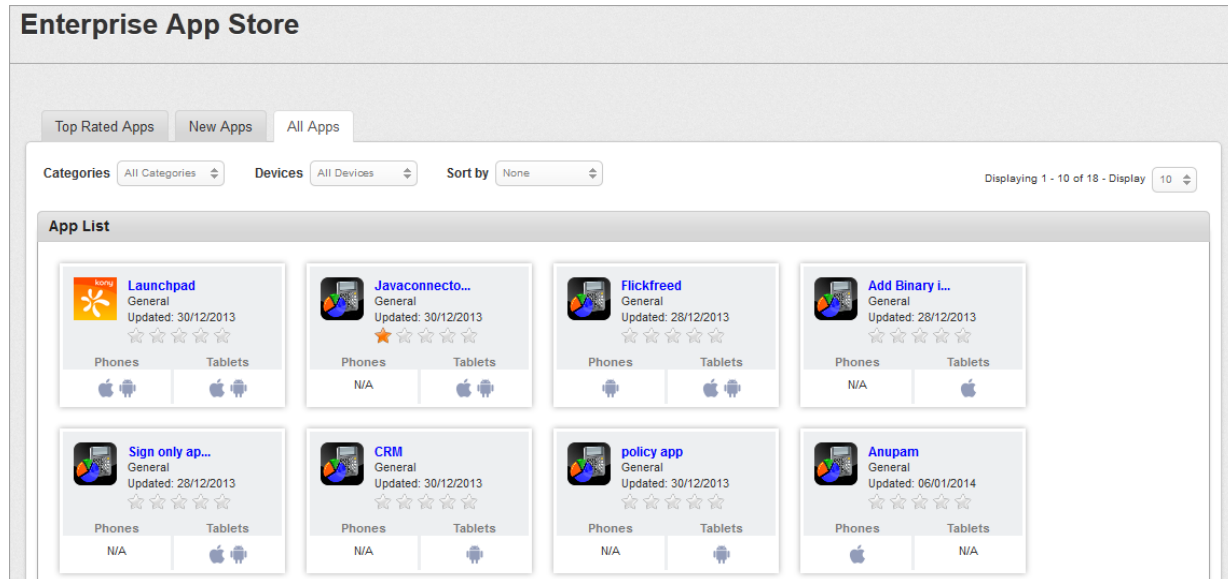
1. **Description**: Enter the comments in the **Description** text box.
2. **Rating**: Select the number of star icons to rate the app.
3. Click the **Rate and Comment** button to save the details.

The added comment appears in the list. The recent comment becomes the foremost comment in the list.

Click the **View More Comments** button to view other review comments posted by other users.

12.2.3 All Apps

The All Apps page makes all the internal apps available to users. This allows a user to browse a list of apps that relate to a specific category or a device type.



You can perform the following activities from the All Apps page:

- [Searching for Enterprise Apps](#)
- [Rate and Comment your App](#)

12.2.4 Searching for Enterprise Apps

You can search a desired app through search filters available. You can apply a single or a combination of search filters to define the search criteria and get the refined outcome.

Important: When you search for an app, all apps and categories which contain your search terms (including numbers) in their name, or version number will appear in the search results.

Enter or select details for the following search filters:

1. **Categories:** Select the required category from the drop-down list.
2. **Devices:** Select the required device type, such as Android Phone from the drop-down list.
3. **Sort By:** Select the required option, such as Top rated from the drop-down list.
4. According to your search filters criteria, the list view is updated with respective enterprise app details. By default, the list view displays ten enterprise apps according to Display settings, which you can modify through **Display** drop-down list. You can also scroll the list view through **Previous** and the **Next** button.

12.2.5 Rate and Comment your App

To rate and comment your app, follow these steps:

1. **Description:** Enter the comments in the Description text box.
2. **Rating:** Select the number of star icons to rate the app.
3. Click the **Rate and Comment** button to save the details.

The added comment appears in the list. The recent comment becomes the foremost comment in the list.

Click the **View More Comments** button to view other review comments posted by other users.

12.3 Devices

The Device List page enables you to get all the information about devices and perform different activities to manage them efficiently. Various fields on this page are, Ownership .

The Devices section pertains to role based device registration. Role based access control offers users their own specialized console to perform their job.

From the **Enterprise App Store** section, click the **My Devices** from the left panel. The **Device List** page appears with a list of the registered devices. The list view displays a list of all the devices along with other details. You can search the devices based on each column and also sort on each column.

| Device Name ▼ | Ownership | Compliance | OS | Last Check-in | Date Enrolled |
|--------------------|-----------|------------|---------------|---------------------------|---------------------------|
| Search Device Name | All | All | Search OS | All | All |
| admin GT-9300 | Employee | Compliant | Android 4.1.2 | 13 Sep, 2013 21:50:54 IST | 13 Sep, 2013 21:33:06 IST |

The Device List view displays the following columns:

| Columns | Description |
|-------------|---|
| Device Name | Displays the unique identification name of the device. |
| Status | Displays the current status of the device, for example, Registered, Deactivated, Retired, Lost, or Control Removed. |
| OS | Displays the operating system to which the device supports. |
| Last Login | Displays when the device was last checked in to EMM Console, for example, Today, Yesterday or Last 7 Days. |

| Columns | Description |
|---------------------|---|
| Date of First Login | Displays when the device was registered to EMM Console, for example, Today, Yesterday or Last 7 Days. |

You can perform the following activities from this page:

- [Searching for an Enrolled Device](#)

12.3.1 Searching for an Enrolled Device

You can search a desired device through search filters available. You can apply a single or a combination of search filters to define the search criteria and get the refined outcome. To search for a device, do the following:

| Device Name ▼ | Ownership | Compliance | OS | Last Check-in | Date Enrolled |
|---|-----------|------------|--|---------------------------|---------------------------|
| <input type="text" value="Search Device Name"/> | All ▾ | All ▾ | <input type="text" value="Search OS"/> | All ▾ | All ▾ |
| admin GT-I9300 | Employee | Compliant | ◆ Android 4.1.2 | 13 Sep, 2013 21:50:54 IST | 13 Sep, 2013 21:33:06 IST |

Previous Page {1/1} Next

1. Enter or select details for following search filters:

- Device Name:** Enter partial or a complete device name in the **Search Devices** text field.
- Ownership:** Select the category of the owner from the drop-down list.

Provides a list about ownership details of the device, for example, Corporate Owned, Employee Owned or Shared.

- OS:** Enter desired operating system name in the **Search OS** text field.
- Last Login:** Select the date on which the device is last checked-in to EMM from the drop-down list.

Provides a list of dates the policy was last checked-in, for example, Today, Yesterday, Last 7 Days, Last 30 Days and Last 90 days.

- e. **Date of First Login:** Select the date on which the device is registered to EMM from the drop-down list.

Provides a list of dates the policy was registered, for example, Today, Yesterday, Last 7 Days, Last 30 Days and Last 90 days.

2. According to your search filters criteria, the list view is updated with respective app details. By default, the list view displays ten apps according to Display settings, which you can modify through Display drop-down list. You can also scroll the list view through Previous and the Next button.

12.4 Content Management - Self-Service Console

Through the self-service console, users can access their user space, enterprise space, and shared space.

- The User Space tab is the home folder for all user uploaded content. A user can directly upload files in the User Space tab or organize these files into folders.
- Enterprise space contains folders and files targeted at a user by an administrator. A user can view and download shared files. A user cannot alter the folder structure, or delete any files or folders.
- The shared space tab displays all files and folders shared with a user by other users. A user can view the content shared but cannot delete any files or folders from the shared space.

12.5 Folders

Folders help organize the content files available into logical groups. Every managed content file should be associated with a folder. Distributing the content to an appropriate audience is easier through a folder.

A managed content file can be added to multiple folders or none at all. If a file is not associated with any folder, it is not targeted to any users and is unavailable to them. Policies do not apply to such files. In the self-service console, a file cannot exist without a folder.

You can do the following with/to folders:

- Create a new folder
- Delete a folder
- Add content to a folder
- Modify content in a folder
- Share content with other users

The Folders details page displays three tabs.

- **User Space:** A user can create and manage folders and files in user space.
- **Enterprise Space:** Enterprise space displays folders created by an administrator and targeted to a user. A user can view folders and file names available in the enterprise space.
- **Shared Space:** Shared space contains files and folders shared with a user by other users from their user space.

12.5.1 User Space

User space contains details of content uploaded by a user.

The screenshot displays the 'User Space' interface. At the top, there are three tabs: 'User Space', 'Enterprise Space', and 'Shared Space'. Below the tabs is a '+ New Folder' button and a display count 'Displaying 1 - 1 of 1 - Display 10'. A table with columns 'Folders Name', 'Path', 'Last Modified On', and 'Action' is shown. The table contains one row for a folder named 'Allies' with path '/' and last modified on '02 Dec, 2014 08:53:16 EST'. Below the table are 'Delete', 'Previous', 'Page {1/1}', and 'Next' buttons.

| | Folders Name | Path | Last Modified On | Action |
|--------------------------|----------------|-------------|---------------------------|---------------|
| <input type="checkbox"/> | Search Folders | Search Path | All | |
| <input type="checkbox"/> | Allies | / | 02 Dec, 2014 08:53:16 EST | Select Action |

- **Create Folder:** Create a folder with this button.
- **Folders Name:** Displays the name of the folder.
 - **Search Folders:** Use a folder's name to search for the folder.
- **Path:** Displays the location of the folder.
 - **Search Path:** Use the path of a folder to search for the folder.
- **Last Modified By:** Displays the name of the user who last modified the folder.
 - **Search Last Modified By:** Search for a folder using the name of the user who last modified the folder.
- **Last Modified On:** Displays date and time folder was last modified.
 - **All:** Search for a folder using this feature. Options range from Today to Last 30 days.

- **Action:** A list of actions you can take on the folder.
 - **Select Action:** Options are Copy To and Move To.
- **Delete:** You can delete a folder.
- **Previous:** Clicking this button will take you to the previous page.
- **Next:** Clicking this button takes you to the next page.

12.5.1.1 User Folder Details

The User Folder details page consists of actions a user can take on a folder and also provides details about the folder.

Folder details are available in three tabs.

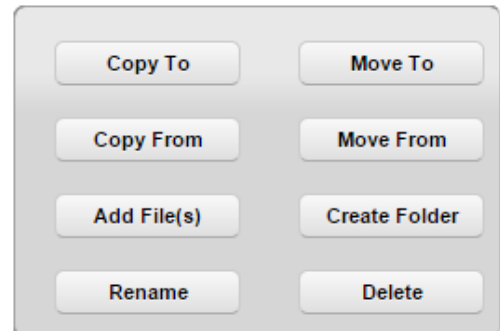
- Details
- Content
- Sharing

/Allies

**Allies**

Last Modified By: Han

Last Modified On: 02 Dec, 2014 08:53:16 EST



Details Content Sharing

Folder Name Allies

Path /

Description

For user space folders, you can take the following actions.

- **Copy to** - You can copy a folder to a destination you specify. All internal files and folders of the folder are also copied to the new destination. If a folder with same name exists in the destination folder, the new folder will be renamed with a suffix (1). Only the latest version of the file is copied.
- **Move to** - You can move a folder to a destination you specify. All internal files and folders of the folder are also moved to the new destination. If a folder with same name exists in the destination folder, the new folder will be renamed with a suffix (1). All versions of the file are moved.

- **Copy From** - The files or folders from the source location are copied to the current folder. All sub-folders and files are also copied. If a folder with the same folder name is in the destination, the new folder will be renamed with a suffix (1). Only the latest version of the file is copied.
- **Move From** - The files or folders from the source location are moved to current folder. All sub folders and files are also moved. If a folder with same name exists in the destination folder, the new folder will be renamed with a suffix (1). All versions of the file are moved.
- **Add Files** - A new file can be added to the current folder.
- **Create Folder** - A new folder can be created within the current folder.
- **Rename** - The folder can be renamed. If a folder with the same folder name is already in the destination, the new folder will be renamed with a suffix (1).
- **Delete** - Folders can be deleted. If a folder is deleted, the folder is removed from all locations including the device.

Details Tab

The Details tab displays details about the folder.

- **Folder Name:** Displays the name of the folder.
- **Path:** Displays the location of the folder.
- **Description:** Displays a brief description of the folder by the user.

Content Tab

The Content tab displays files and folders within the folder.

| Details Content Sharing | | | | | | |
|---|--------|---------|------------------|----------------------------|---------------|--|
| File / Folder Name | Format | Path | Last Modified By | Last Modified On | Actions | |
| <input type="checkbox"/> Search Files/Folders All Search Path Search Last Modified By All | | | | | | |
| <input type="checkbox"/> Chewbacca | pdf | /Allies | Han | 02 Dec, 2014 08:54:22 E ST | Select Action | |
| <input type="checkbox"/> Leia | pdf | /Allies | Han | 02 Dec, 2014 08:54:22 E ST | Select Action | |
| <input type="button" value="Delete"/> Previous Page {1/1} Next | | | | | | |

- **File/Folder Name:** Displays the name of the file/ folder.
 - **Search Files/Folders:** Using the Search Files / Folders feature, you can search for files/folders by the name of the file/folder.
- **Format:** Displays the format of the files.
 - **All:** Using this list, you can search for files based on their specific format. A list contains all allowed file formats.
- **Path:** Displays the location of the file/folder.
 - **Search Path:** If you know the path of any file/folder, you can search for the path using this feature.
- **Last Modified By:** Displays the name of the user who last modified the file/folder.
 - **Search Last Modified By:** If you know the last user who modified the file/folder, you can search for the file/folder using this feature.
- **Last Modified Date:** Displays file/folder last modified date and time.
 - **All:** You can search for a file/folder based on when it was last modified using this feature. Options range from Today to Last 30 days.
- **Action:** Provides you with list of actions you can take on the file/folder.
 - **Select Action:** Options are Copy To and Move To.
- **Delete:** Delete a file/folder.

- **Previous:** Clicking this button will take you to the previous page.
- **Next:** Clicking this button will take you to the next page.

Sharing Tab

Use the Sharing tab to share content with other users and groups.

The screenshot shows the 'Sharing' tab interface. At the top, there are three tabs: 'Details', 'Content', and 'Sharing'. Below the tabs, there are two input sections: 'Add Users' and 'Add Groups'. Each section has a text input field with a placeholder (e.g., 'Select users') and an 'Add' button. Below these is a 'Target' section with a checkbox, a 'Delete' button, and the text 'No results found'. The 'Inherited Sharing' section has a table with columns 'Target' and 'Inherited From', and the text 'No results found' below it.

- **Add Users:** Enter names of users with whom you want to share the content.
- **Add Groups:** Enter names of groups with which you want to share the content.
- **Target:** This feature displays details of users and groups that receive shared content.
- **Inherited Sharing:** This feature displays user or group targets inherited from parent folders.
- **Target:** This feature displays the details of user or group that inherited the sharing.

- **Inherited From:** This feature displays details of the folder from which the user or group inherited sharing.

12.5.2 Enterprise Space

Enterprise space displays enterprise content created by an administrator and targeted to the user. A user can view folders and file names available in the enterprise space tab.

Enterprise Space

[Enterprise Space](#) > [Empire](#)

/Empire



Empire

Last Modified By: admin

Last Modified Date: 02 Dec, 2014 09:09:42 EST

Displaying 1 - 2 of 2 - Display ▼

| File / Folder Name | Format | Last Modified By | Last Modified On |
|---|------------------------------------|--|------------------------------------|
| <input type="text" value="Search Files / Folders"/> | <input type="text" value="All"/> ▼ | <input type="text" value="Search Last Modified By"/> | <input type="text" value="All"/> ▼ |
| Yoda | pdf | admin | 02 Dec, 2014 09:10:25 EST |
| Luke | pdf | admin | 02 Dec, 2014 09:10:25 EST |

- **File/Folder Name:** Displays the name of the file/ folder
 - **Search Files/ Folders:** Search for files/folders by the name of the file/folder.
- **Format:** Displays the format of the files.
 - **All:** Search for files based on their specific format. A list contains all allowed file formats.
- **Last Modified By:** Displays the name of the user who last modified the file/folder.
 - **Search Last Modified By:** If you know the last user who modified the file/folder, you can search for the file/folder using this feature.

- **Last Modified On:** Displays file/folder last modified date and time.
 - **All:** You can search for a file/folder based on when it was last modified using this feature. Available options range from Today to Last 30 days.
- **Delete:** Delete a file/folder.
- **Previous:** Clicking this button takes you to the previous page.
- **Next:** Clicking this button takes you to the next page.

12.5.3 Shared Space

The Shared Space contains files and folders shared with the user by other users from their user space.

User Space Enterprise Space **Shared Space**
Displaying 1 - 2 of 2 - Display

| File / Folder Name | Format | Shared By | Last Modified On |
|---|----------------------------------|---|----------------------------------|
| <input type="text" value="Search Files / Folders"/> | <input type="text" value="All"/> | <input type="text" value="Search Shared By"/> | <input type="text" value="All"/> |
| Yoda | pdf | Leia | 02 Dec, 2014 09:20:54 EST |
| Allies | Folder | Leia | 02 Dec, 2014 09:20:43 EST |

Page {1/1}

- **File/Folder Name:** Displays the name of the file/ folder.
 - **Search Files/ Folders:** Using Search Files / Folders feature, you can search for files/folders by the name of the file/folder.
- **Format:** Displays the format of the files.
 - **All:** Using this list, you can search for files based on their specific format. A list contains all allowed file formats.

- **Shared By:** Displays the name of the user who last shared the content.
 - **Search Shared By:** If you know the user who shared the content with you, you can search for the file/folder using this feature.
- **Last Modified On:** Displays last modified date and time. for the file/folder.
 - **All:** You can search for a file/folder based on when it was last modified using this feature. Options range from Today to Last 30 days.
- **Previous:** Clicking this button takes you to the previous page.
- **Next:** Clicking this button takes you to the next page.

12.6 Applying Features of the Self-Service Console

12.6.1 How to Create a New Folder

To create a new folder, follow these steps:

1. In EMM Self-Service Console, click **Content**. The User Space tab appears.
2. Click **Create Folder**. The Add a Folder dialog appears.
3. In the **Folder Name** text box, enter a name for the folder.
4. In the **Description** text box, enter a description about the folder.
5. Click **Create**. A success message appears.
6. Click **OK**. The User Space page appears with newly created folder details.

12.6.2 How to Search Folders

To search for folders, follow these steps:

1. In EMM Self-Service Console, click **Content**. The Content page appears.
2. In **Search Folders** text box, enter the name of the folder you want to search. Search results turn up a list of folders that match the details you entered.
3. Select the folder you want to open.

12.6.3 How to Search for a Folder by its Path

To search for a folder by its path, follow these steps:

1. In EMM Self-Service Console, click **Content**. The Content page appears.
2. In the **Search Path** text box, enter the name of the path you want to search. Search results turn up a list of folders in paths that match the details you entered.
3. Select the folder in the path you want to open.

12.6.4 How to Search for a Folder Using Last modified By

To search for a folder Using last modified by feature, follow these steps:

1. In EMM Self-Service Console, click **Content**. The Content page appears.
2. In the **Search Last Modified by** text box, enter the name of the user who last modified the folder. A list of folders last modified by the user appears.
3. Select the folder you want to open.

12.6.5 How to Search for a Folder by Last Modified Date

To search for a folder by the last modified date feature, follow these steps:

1. In EMM Self-Service Console, click **Content**. The Content page appears.
2. In the **Search Last Modified Date** text box, enter the date the folder was last modified. A list of folders last modified on the specified date appears.
3. Select the folder you want to open.

12.6.6 How to Copy a Folder to Another Location

To copy a folder to another location, follow these steps:

1. In EMM Self-Service Console, click **Content**. The Content page appears.
2. Click on any folder. The Folder details page appears.
3. Click **Copy To**. Copy Folder window appears.
4. In the Destination Folder text box, enter the name of the destination folder.
5. Click the folder name to select the folder, and then click **Copy**.
6. A **Copy to Successful** message appears. Click **OK**.

12.6.7 How to Move a Folder

To move a folder from one location to another, follow these steps:

1. In EMM Self-Service console, click **Content**. The Content page appears.
2. Click on any folder. The Folder details page appears.
3. Click **Move To**. The Move Folder window appears.
4. In the **Destination Folder** text box, enter the name of the folder you selected. Folder name appears.

5. Click the folder name to select the folder, and then click **Move**.
6. A **Move to Successful** message appears. Click **OK**.

12.6.8 How to Copy a Folder From Another Folder

To Copy a folder from, another folder, follow these steps:

1. In EMM Self-Service console, click **Content**. The Content page appears.
2. Click on any folder. The Folder details page appears.
3. Click **Copy From**. The Copy From window appears.
4. In the **Source Folder(s)** text box, enter the name of the folder you want to copy from. The Folder name appears.
5. Click the folder name to select the folder.
6. In the **Source File(s)** text box, enter the name of the file you want to copy. The file name appears.
7. Click the file name to select the file and then click **Copy**.
8. A **Copy From Successful** message appears. Click **OK**.

12.6.9 How to Change a Folder's Location

To move a folder from one location to another, follow these steps:

1. In EMM Self-Service console, click **Content**. The Content page appears.
2. Click on any folder. The Folder details page appears.
3. Click **Move From**. The Move From window appears.

4. In the **Source Folder(s)** text box, enter the name of your designated source folder. The folder name appears.
5. Click the folder name to select the folder.
6. In the **Source File(s)** text box, enter the name of the file you want to move. The file name appears.
7. Click the file name to select the file, and then click **Move**.
8. A **Move From Successful** message appears. Click **OK**.

12.6.10 How To Add Files

To add file(s) to a folder, follow these steps:

1. In EMM-Self Service console, click **Content**. The Content page appears.
2. Click on any folder. The Folder details page appears.
3. Click **+ Add File(s)**. The Add File(s) dialog appears.
4. Select file(s). Click to add, or Drag and drop.
5. Click **Add**. The Open dialog appears.
6. Navigate to the location where the file you want to upload is located, and select the file. Or drag and drop the file you want to add.
7. Click **Upload**.
8. In the **Description** text box, enter a brief description about the document.
9. Click **Save**. The new file is uploaded to the system in the folder you have specified.

12.6.11 How To Create a Folder

To create a new folder, follow these steps:

1. In EMM Self-Service console, click **Content**. The Content page appears.
2. Click on any folder. The Folder details page appears.
3. Click **Create Folder**. The Add Folder dialog appears
4. In the **Folder Name** text box, enter a name for the folder.
5. In the **Description** text box, enter a description about the folder.
6. Click **Create**. A success message appears.
7. Click **OK**. The Folders page appears with the newly created folder in it.

12.6.12 How To Rename a Folder

To rename a folder, follow these steps:

1. In EMM Self-Service Console, click **Content**. The Content page appears.
2. Click on any folder. The Folder details page appears.
3. Click **Rename**. The Rename Folder window appears.
4. In **New Folder Name** text box, enter the new name for the folder, and then click **Rename**.
5. Click **Save**. A success message appears.
6. Click **OK**.

12.6.13 How to Delete a Folder

To delete a folder, follow these steps:

1. In EMM Self-Service console, click **Content**. The Content page appears.
2. Click on any folder. The Folder details page appears.
3. Click **Delete**. The Delete Folder Confirmation window appears.

4. Click **OK** to delete the folder. A success message appears.
5. Click **OK**.

Note: If a folder is currently shared, a user must confirm that the folder shared is also removed.

12.7 File Details Page

The File Details page contains three tabs by default. If there is more than one version of the file, a Past Version tab is available.

- **Description tab:** The description tab displays details of the file, the path it is in. The tab also contains a brief description about the file as entered by the user who uploaded the file.
- **Current Version tab:** The current version tab displays the version of the file, name of the user who updated it, and the date on which the document was last updated. The Download button allows you to download the current version to your computer.
- **Past Version tab:** This tab is visible only when more than one version of a file exists. The past version tab displays various past versions of the file, name of the user who updated it, and the date on which the document was last updated. The download button allows you to download the current version to your computer. Using the Make Current button, you can make the specific version you are viewing as the current version.
- **Sharing tab:** The Sharing tab displays information about various users and groups with whom a user shares content. The sharing tab also displays details of sharing inherited . You can add users, add groups, and delete sharing with targeted users and groups.
- **Save & Exit:** The Save & Exit feature allows you to save modifications you made on the Files Details page and exit to the Files page.
- **Save & Continue:** The Save & Continue feature allows you to save modifications you made on the Files Details page and remain on the same page.

- **Cancel:** The cancel button allows you to void all the modifications you make in the Files Details page.

12.8 Applying Actions to Files

12.8.1 How to Update a File

To update a file, follow these steps:

1. In EMM Self-Service Console, click **Content**. The Content page appears.
2. Click on any folder. The Folder details page appears.
3. Click on a file. The File details page appears.
4. Click **Update**. The Update File window appears.
5. From Update File, click **Add**. The Open window appears.
6. Navigate to the file's location, and then click the file.

Note: You can only update a file if both versions have the same name and format. If you upload a file with a different name, the system asks to rename the file on the server with the existing name. If you accept the change, the file is updated and renamed. If you decline, the update fails.

7. Click **Save**. A success message appears.
8. Click **OK**.

12.8.2 How to Rename a File

To rename a file, follow these steps:

1. In EMM Self-Service Console, click **Content**. The Content page appears.
2. Click on any folder. The Folder details page appears.
3. Click on a file. The File details page appears.
4. Click **Rename**. The Rename File window appears.
5. In the **New File Name** text box, enter the new name for the file, and then click **Rename**.
6. Click **Save**. A success message appears.
7. Click **OK**.

12.8.3 How to Copy a File

To copy a file, follow these steps:

1. In EMM Self-Service Console, click **Content**. The Content page appears.
2. Click on any folder. The Folder details page appears.
3. Click on a file. The File Details page appears.
4. Click **Copy**. The Copy File window appears.
5. In **Copy File** text box, enter the name of the folder you want to copy the file into.
6. The folder name appears. Click to select the folder.
7. Click **Copy**. A success message appears.
8. Click **OK**.

12.8.4 How to Move a File

To move a file from location to another, follow these steps:

1. In EMM Self-Service Console, click **Content**. The Content page appears.
2. Click on any folder. The Folder details page appears.
3. Click on a file. The File Details page appears.
4. Click **Move**. The Move File window appears.
5. In the **Move File** text box, enter the name of the folder you want to move the file into.
6. The folder name appears. Click to select the folder.
7. Click **Move**. A success message appears.
8. Click **OK**.

12.8.5 How to Delete a File

You can delete a file in the Files page and in the File Details page.

In Files page, follow these steps:

1. Select the file you want to delete.
2. Click **Delete** icon at the bottom of the list of files to delete. A warning message appears.
3. Click **Yes** to delete the file. A success message appears.

Note: If the file is currently shared or targeted, a user needs to confirm removal of file from sharing and targeting.

4. Click **OK**.

In the Files Details page,

1. Click on a file. The File Details page appears.
2. Click **Delete**. A warning message appears.
3. Click **Yes** to delete the file. A success message appears.
4. Click **OK**.

12.8.6 To download a Previous Version

To download a previous version of a file, follow these steps:

1. In EMM Self-Service Console, click **Content**. The Content page appears.
2. Click on any folder. The Folder details page appears.
3. Click Content tab. The Files in the folder appear.
4. Click on a file. The File Details page appears.
5. In the **Past Version** tab, click in the **Version** text box. A search box opens.
6. In the search box, enter the version of the document you want to view. A list of available versions appears.
7. Click the version you want to download. The Download button is activated.
8. Click **Download**. The file downloads.

12.8.7 How to Make a Previous Version as Current

To make a previous version of a file as the current version, follow these steps:

1. In EMM Self-Service Console, click **Content**. The Content page appears.
2. Click on any folder. The Folder details page appears.
3. In the **Past Version** tab, click in the Version text box. A search box opens.

4. In the search box, enter the version of the document you want to view. A list of available versions appears.
5. Click the version you want to make current. The make current button is activated.
6. Click **Make Current**. The Make Current window appears.
7. Click **Yes**. A success message appears.
8. Click **OK**.

Note: Note that the version number is incremental. For example, if the file has three versions and you chose to make the second version as current, the new version is No. 4.

12.8.8 How to Share a File

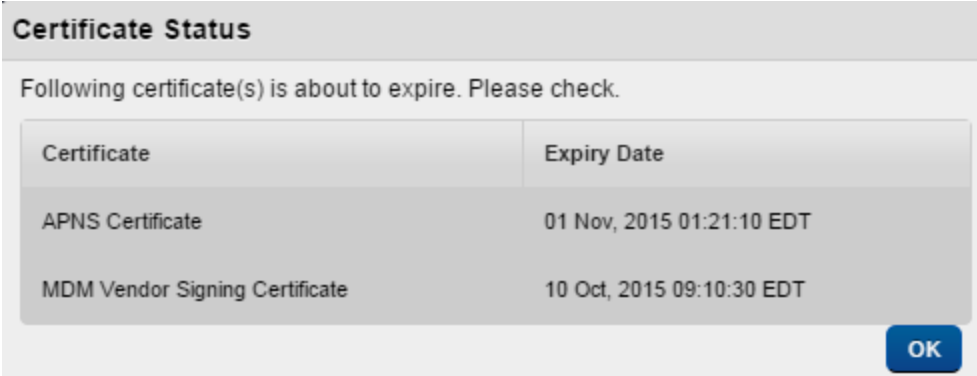
To share a file, follow these steps:

1. In EMM Self-Service Console, click **Content**. The Content page appears.
2. Click on the folder from where you want to share content. The Folder details page appears.
3. Click on a file you want to share. The File details page appears.
4. Click the **Sharing** tab. Sharing tab details appear.
5. To add a user, in the **Add User** text box, add the name of the user with whom you want to share content. Details of the user appear.
6. To add a group, in the **Add Group** text box, add the group name you want to share the content with. Details of the group appear.
7. Click **Add**. Content is shared with the user/group, and details appear in the Target section.
8. Click **Save & Exit**.

13. Dashboard

The Dashboard is a visual summary of information. System administrators can use the dashboard to get a comprehensive graphical view of total registered devices, total non-compliant devices and app downloads.

The Dashboard is the first page you visit after logging in. you will initially see a **Certificate Status** box.

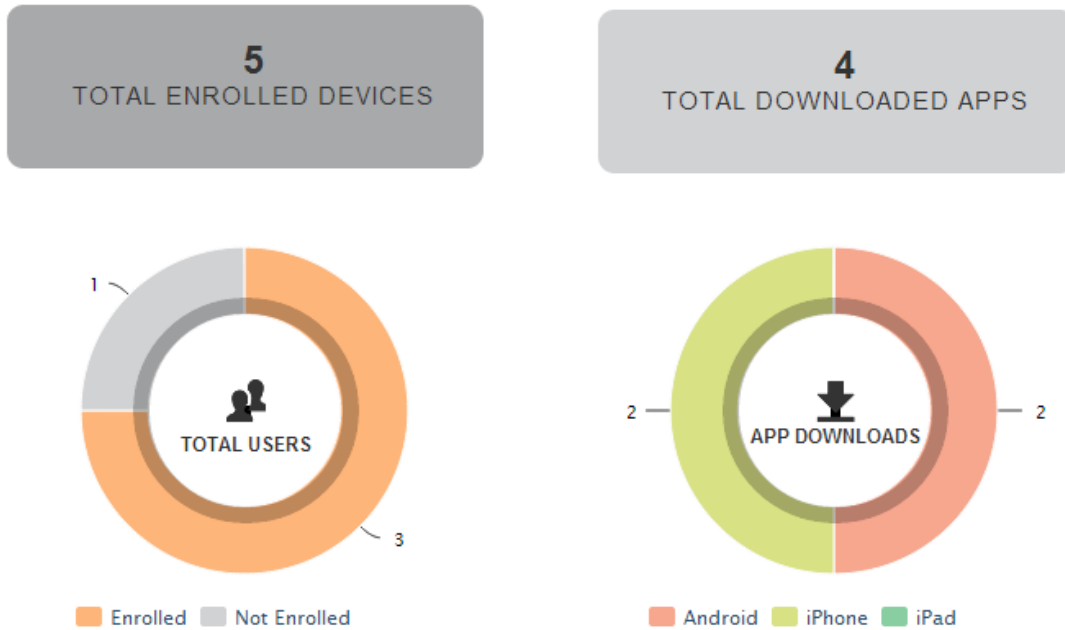


| Certificate | Expiry Date |
|--------------------------------|---------------------------|
| APNS Certificate | 01 Nov, 2015 01:21:10 EDT |
| MDM Vendor Signing Certificate | 10 Oct, 2015 09:10:30 EDT |

The Certificate Status screen displays information on all certificates that are about to expire. Based on the information on a Certificate Status screen, an administrator can renew certificates before they expire.

Expiry dates for all certificates used across the Kony Management suite are calculated and notifications are sent. The first notification is sent four weeks before the certificate expiry date. A second notification is sent to the administrator two weeks before the certificate expiry date. A notification is sent every day in the last week of certificate expiration.

Dashboard



The following table describes the components of the Dashboard:

| Component | Description |
|-----------------------------------|--|
| Total Registered Devices Label | This label displays the total number of the enrolled registered devices to EMM. For example, the label in above image indicates that total 19 devices are registered on that particular day. |
| Total Non-Compliant Devices Label | This label displays the total number of non-compliant devices. For example, if the label displays 1 device. It indicated that only once device is out of compliance. |

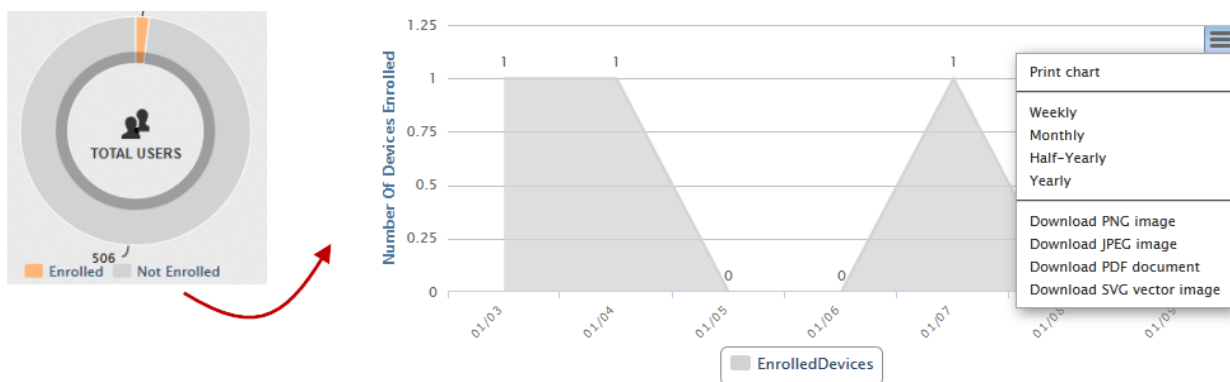
| Component | Description |
|-----------------------------|--|
| Total Downloaded Apps Label | This label displays the total number of downloaded apps on devices. Important: The App Downloads count will increase when an app policy is targeted to a user or group irrespective of whether the app (publicly available on a store) is actually installed on the device or not. |
| Pie Charts | A circular chart that represents the distribution or participation of each item (represented by a slice) of a certain total that is represented as the overall pie value. For example, Registration Summary Chart, Compliance Summary Chart, and App Downloads Summary Chart. |

You can perform the following activities from the Dashboard:

- [Viewing the Enrollment Summary Chart](#)
- [Viewing the Compliance Summary Chart](#)
- [Viewing the App Downloads Summary Chart](#)

13.1 Viewing the Enrollment Summary Chart

Enrollment Summary Chart displays the number of Users with registered devices versus Users with not registered devices. Click the pie chart to view Enrollment Summary chart.



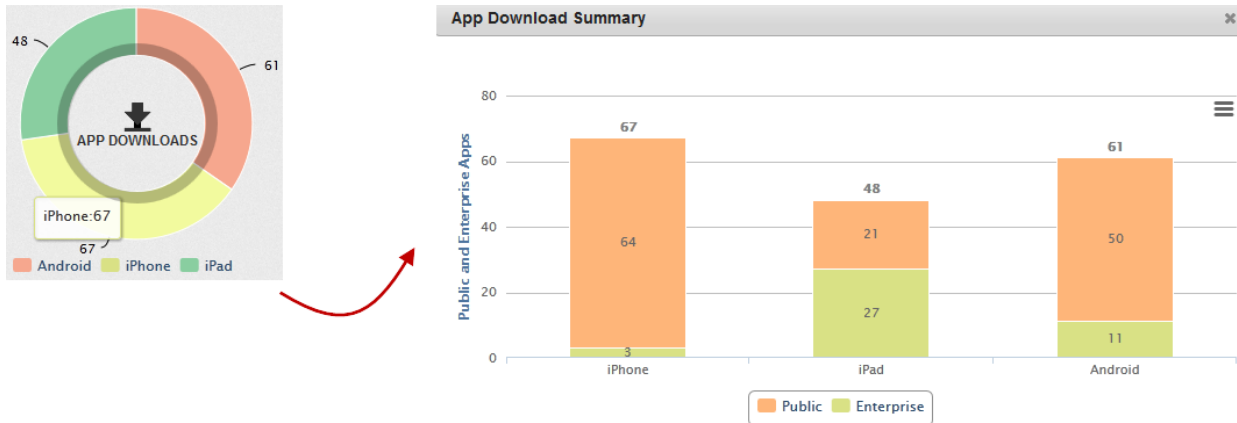
The Enrollment Summary chart includes the following components:

| Components | Description |
|--------------------|--|
| Color Codes | The color codes indicates the distribution of each item (represented by a slice) For example, in above pie chart, orange color represents the Users with enrolled devices and blue color represents the Users with not enrolled devices |
| Chart Context Menu | Double-click the pie chart to view the chart details. Click the Chart Context menu in the top right corner of the chart. You get following options: Click the Chart Context menu to <ul style="list-style-type: none"> • Print the chart. • Download the chart in PNG, JPEG or SVG vector format. • Download the chart in PDF format. |
| Chart Details | <ul style="list-style-type: none"> • By default, the chart displays the one week activities. You can view the chart based on Monthly, Half yearly or yearly basis. • The X axis represents the specific dates on which the devices are enrolled. • The Y axis represents the no of enrolled devices. |

| Components | Description |
|---------------|--|
| Color Codes | The color codes indicates the distribution of each item (represented by a slice) |
| Chart Details | Double-click the pie chart to view the Reasons for Compliance Failure chart details. |

App Download Summary Chart displays the number of downloaded apps for all the supporting platforms. This shows the total number of app downloads from the system. This includes all enterprise apps and any others pushed through the system. Click the pie chart to view App Downloads Summary Chart.

Important: The App Downloads count will increase when an app policy is targeted to a user or group irrespective of whether the app is actually installed on the device.



The App Download Summary chart includes the following components:

| Components | Description |
|---------------|--|
| Color Codes | The color codes indicates the distribution of each item (represented by a slice). |
| Chart details | <p>Double click the pie chart to view the Reasons for Compliance Failure chart details.</p> <ul style="list-style-type: none"> Click the Chart Context menu to <ul style="list-style-type: none"> Print the chart. Download the chart in PNG, JPEG or SVG vector format. Download the chart in PDF format. The X axis represents the platforms. The Y axis represents the Public and the Enterprise apps. |

Note: App Download Summary dashboard displays an incorrect number of downloaded apps due to following reasons.

It also counts apps pushed through the app policy even though apps are not downloaded on a device.

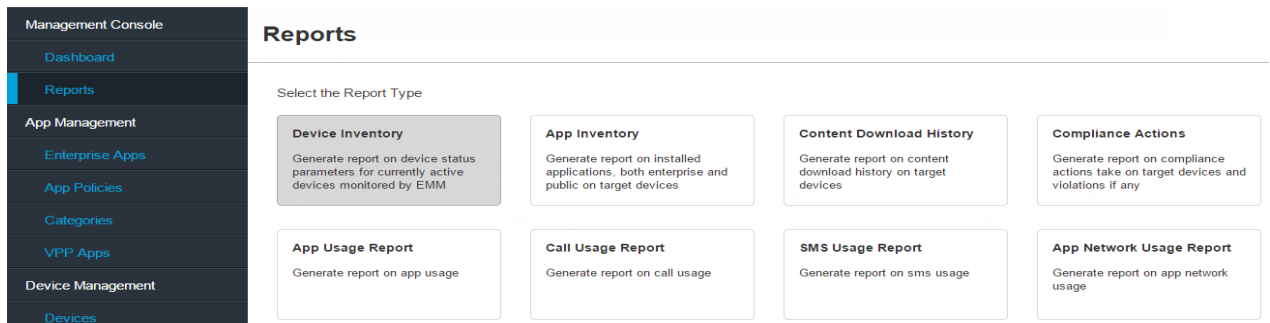
If a user clicks the Cancel button, it increments the download count

13.2 Reports

The Reports feature of Kony Management Suite enables an administrator to create reports about features that are not readily available to an administrator through the dashboard. An administrator can generate reports for the following:

- [Device Inventory](#)
- [App Inventory](#)
- [Content Download history](#)
- [Compliance Actions](#) (supported for only the Enterprise license type).
- [Enterprise App Usage](#) (You must enable the App usage log option in the **Device settings > Usage Configuration** page for this report to appear on the Reports page.)
- [Call Usage](#) (You must enable the Call usage log option in the **Device settings > Usage Configuration** page for this report to appear on the Reports page.)
- [SMS Usage](#) (You must enable the SMS usage log option in the **Device settings > Usage Configuration** page for this report to appear on the Reports page.)
- [Enterprise App Network Usage Report](#) (You must enable the App Network usage log option in the **Device settings > Usage Configuration** page for this report to appear on the Reports page.)
- [User Device Report](#)
- [App Rating Report](#)

The Reports feature is available for all three license types (Enterprise, Simple Authentication, and Store only) of Kony Management Suite. A user can view reports in a web browser or export reports to an external file, such as .csv, .xls, .xlsx, and .pdf formats.



The Reports page displays several report types. Click each report type to open its respective report page. Using the report page, you can specify input and output parameters required for your report and then generate the report.

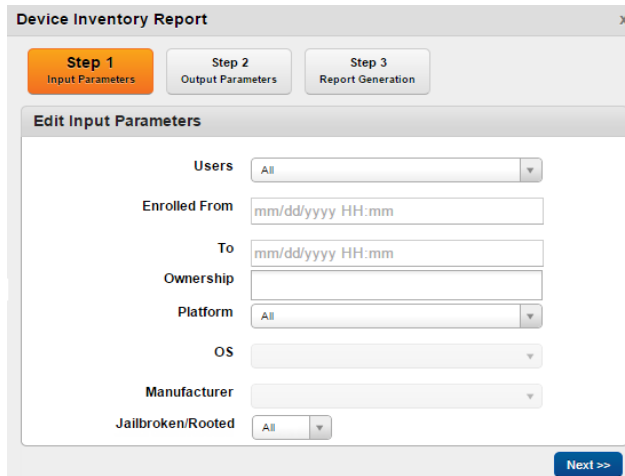
13.2.1 Device Inventory Report

The device inventory reports provides details about device status parameters for currently active devices monitored by Kony Management Suite. You can get device details for all users, any specific user, or any group. The device inventory report is generated instantly and in real time.

To create a device inventory report, follow these steps:

1. In the Kony Management Suite Management console, click **Reports**. The Reports page appears.

2. Click **Device Inventory**. The Device Inventory Report page appears.



The screenshot shows a web application window titled "Device Inventory Report" with a close button (X) in the top right corner. At the top, there are three step indicators: "Step 1 Input Parameters" (highlighted in orange), "Step 2 Output Parameters", and "Step 3 Report Generation". Below this is a section titled "Edit Input Parameters" containing several form fields:

- Users:** A dropdown menu currently set to "All".
- Enrolled From:** A text input field with a date and time format placeholder: "mm/dd/yyyy HH:mm".
- To:** A text input field with a date and time format placeholder: "mm/dd/yyyy HH:mm".
- Ownership:** A text input field.
- Platform:** A dropdown menu currently set to "All".
- OS:** A dropdown menu.
- Manufacturer:** A dropdown menu.
- Jailbroken/Rooted:** A dropdown menu currently set to "All".

A "Next >>" button is located at the bottom right of the form area.

3. From the **Users** list, select **All** or **Specific**. If you select All, new fields do not appear. If you select **Specific**, new fields (Groups and Users) appear.
4. To create a device inventory report for a specific group, enter the group name in the **Groups** field.
5. To create a device inventory report for a specific user, enter the user name in the **Users** field.
6. In the **Enrolled From** field, select the enrollment from date and time.
7. In the **To** field, select the enrollment until date and time.
8. From the **Ownership** field, select the device ownership. Options are, **Corporate**, **Employee**, and **Shared**.
9. From the **Platform** list, select the platforms for which you want the Device Inventory Report. Based on the platform you select, OS and Manufacturer field options change.
10. From the **OS** list, select the OS version.
11. From the Manufacturer list, select the device manufacturer name.

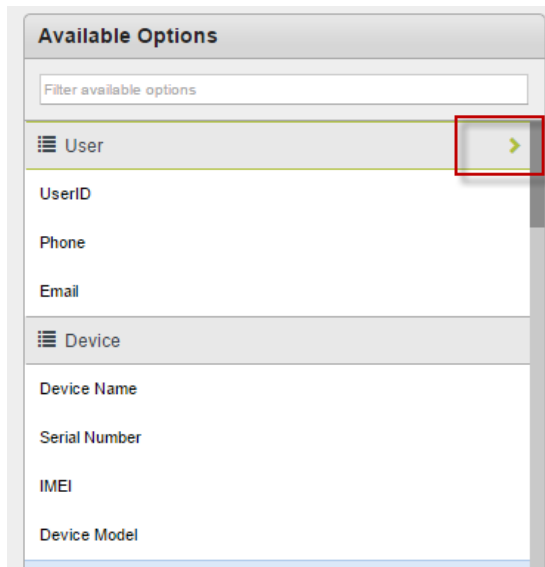
12. In the **Jailbroken/Rooted** list, follow these steps:
 - a. Select **All** if you want to see details of all devices.
 - b. Select **Yes** if you want to view details of devices that are jailbroken or rooted.
 - c. Select **No**, if you do not want to view details of devices that are jailbroken or rooted.
13. Click **Next**. The Output Parameters page appears.

The screenshot shows the 'Device Inventory Report' interface. At the top, there are three steps: 'Step 1 Input Parameters', 'Step 2 Output Parameters' (which is the active step and highlighted in orange), and 'Step 3 Report Generation'. Below the steps, there are two main sections: 'Available Options' and 'Selected Options'. The 'Available Options' section has a search filter and lists parameters under two categories: 'User' (UserID, Phone, Email) and 'Device' (Device Name, Serial Number, IMEI, Device Model, Device Platform, Device OS, Device Status). The 'Selected Options' section lists Device Platform, Device OS, SIM ID, and UDID. At the bottom of the interface, there are '<< Back' and 'Next >>' buttons.

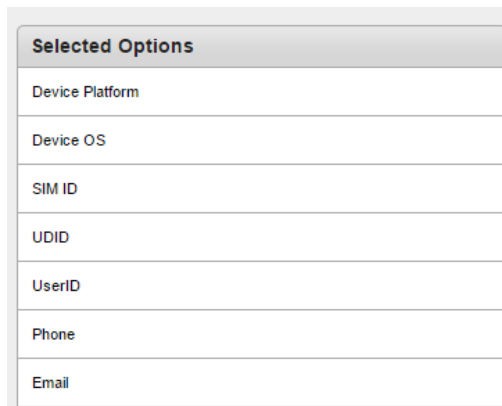
The Output parameters page displays all parameters in two columns: **Available Options** and **Selected Options**. In the Selected options column, some parameters are selected by default.

14. You can choose other parameters from the available options column. Select one of two options:
 - Select parameters group
 - Select individual parameter.

15. To select a parameters group, do the following:
 - a. Hover your mouse on the parameters group name. The select icon appears.

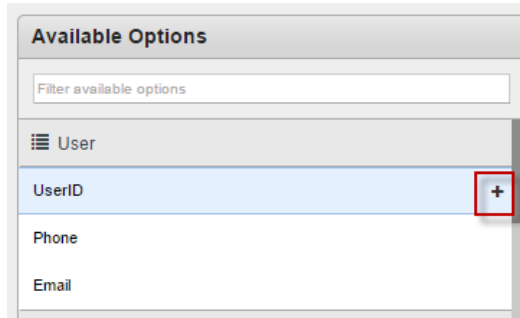


- b. Click the select icon. Selected parameters appear in the selected options column.



16. To select an individual parameter, do the following:

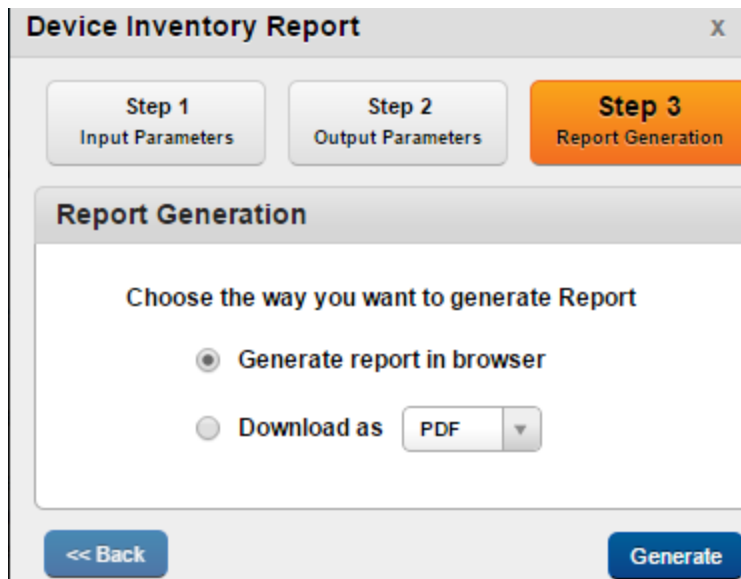
- a. Hover your mouse over the parameter you want to select. A plus sign appears.



- b. Click the plus sign. Selected parameter appears in the selected options column.

17. From Select Output Parameters section, select the output parameters individually or select **Select All Output Parameters**.

18. Click **Next**. The Report Generation page appears.



19. If you want to view the report in a browser, select **Generate report in browser**.

20. If you want to download the report, select **Download as**.

21. If you have selected Download as, select the file type from the **Download as** list. Options are CSV, PDF, XLS and XLSX.
22. Click **Generate**. The report opens in a new browser or downloads in the chosen format.

13.2.2 App Inventory Report

The App Inventory report provides information about applications installed on devices enrolled in the Enterprise Mobile Management console. The report can be generated for all users, any specified user or group, or any specified enterprise app.

Note: To receive this report, the end user must have clicked on the **MyApps** tab in the Enterprise store at least once.

To create an App Inventory report, follow these steps:

1. In Kony Management Suite Management console, click **Reports**. The Reports page appears.
2. Click **App Inventory**. The App Inventory Report page appears.
3. From the **App Type** list, select the app type. Options are **All**, **Enterprise App**, **Personal App**, and **Managed App**.
4. In the **App Name** field, enter the app name.
5. In the **Target User** field, select the target user. Options are **All** and **Specific**. If you select **All**, new fields do not appear. If you select **Specific**, new fields (Groups and Users) appear.
6. To create an app inventory report for any specific group, enter the group name in the **Groups** field.
7. To create an app inventory report for any specific user, enter the user name in the **Users** field.
8. From the **Platform** list, select the platforms for which you want the App Inventory report. Based on the platform you select, OS field options change.
9. From the **OS** list, select the OS version. If the selected platform is **All**, this field is disabled.

10. Click **Next**. The Output Parameters page appears.

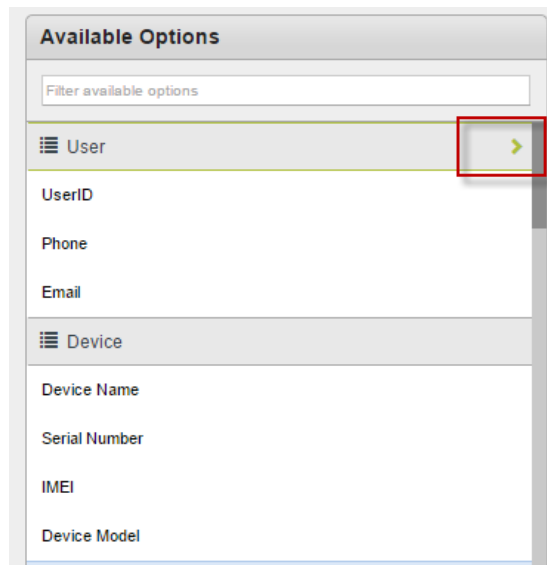
The Output parameters page displays all parameters in two columns: **Available Options** and **Selected Options**. In the Selected options column, some parameters are selected by default.

11. You can choose other parameters from the available options column. You can do that in two ways:

- Select parameters group
- Select individual parameter.

12. To select a parameters group, do the following:

a. Hover your mouse on the parameters group name. The select icon appears.



- b. Click the select icon. Selected parameters appear in the selected options column.

| Selected Options |
|------------------|
| Device Platform |
| Device OS |
| SIM ID |
| UDID |
| UserID |
| Phone |
| Email |

13. To select an individual parameter, do the following:

- a. Hover your mouse over the parameter you want to select. A plus sign appears.

| Available Options |
|--|
| <input type="text" value="Filter available options"/> |
| ☰ User |
| UserID + |
| Phone |
| Email |

- b. Click the plus sign. Selected parameter appears in the selected options column.

14. Click **Next**. The Report Generation page appears.
15. To view the report in a browser, select **Generate report in browser**.
16. To download the report, select **Download as**.
17. If you select Download as, select the file type from the **Download as** list. Options are CSV, PDF, XLS and XLSX.
18. Click **Generate**. The report opens in a new browser or downloads in the format you choose.

13.2.3 Content Inventory Report

The Content Inventory report generates a report on the content download history on targeted devices in Kony Management Suite console.

To create a Content Inventory report, follow these steps:

1. In Kony Management Suite Management console, click **Reports**. The Reports page appears.
2. Click **Content Inventory**. The Content Inventory Report page appears.
3. From the **Target User** list, select **All** or **Specific**. If you select **All**, new fields do not appear. If you select **Specific**, new fields (Groups and Users) appear.
4. To create a content inventory report for any specific group, enter the group name in the **Groups** field.
5. To create a content inventory report for any specific user, enter the user name in the **Users** field.
6. In the **Downloaded From** field, select the downloaded from date and time.
7. In the **To** field, select the downloaded until date and time.
8. From the **Platform** list, select the platforms for which you want the report. Based on the platform you select, OS field options change.
9. From the **OS** list, select the OS version.
10. Click **Next**. The Output Parameters page appears.

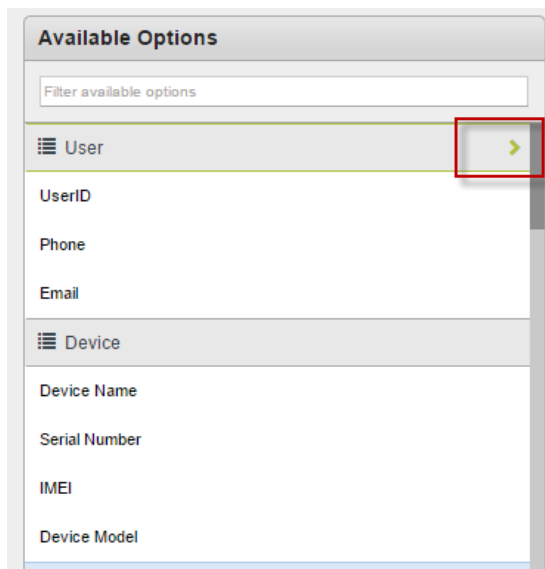
The Output parameters page displays all parameters in two columns: **Available Options** and **Selected Options**. In the Selected options column, some parameters are selected by default (Device Platform, Device OS, SIM ID, and UDID).

11. You can choose other parameters from the available options column. Select one of two options:

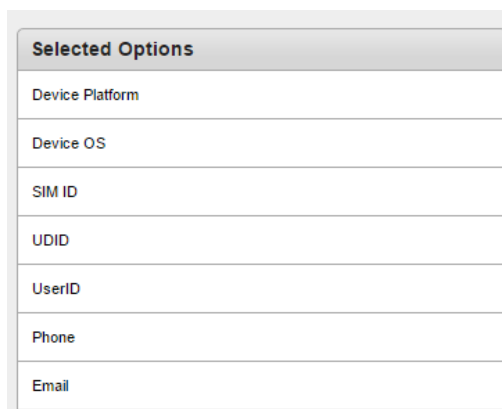
- Select parameters group
- Select individual parameter.

12. To select a parameters group, do the following:

a. Hover your mouse on the parameters group name. The select icon appears.

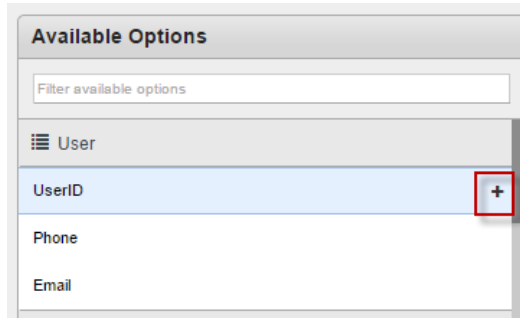


b. Click the select icon. Selected parameters appear in the selected options column.



13. To select an individual parameter, do the following:

a. Hover your mouse over the parameter you want to select. A plus sign appears.



b. Click the plus sign. Selected parameter appears in the selected options column.

14. Click **Next**. The Report Generation page appears.

15. To view the report in a browser, select **Generate report in browser**.

16. To download the report, select **Download as**.

17. If you select Download as, select the file type from the **Download as** list. Options are CSV, PDF, XLS and XLSX.

18. Click **Generate**. The report opens in a new browser or downloads in the format you choose.

13.2.4 Compliance Actions Report

The Compliance Actions report generates a report on compliance actions taken on targeted devices and violations if any, in Kony Management Suite console.

To create a Compliance Actions report, follow these steps:

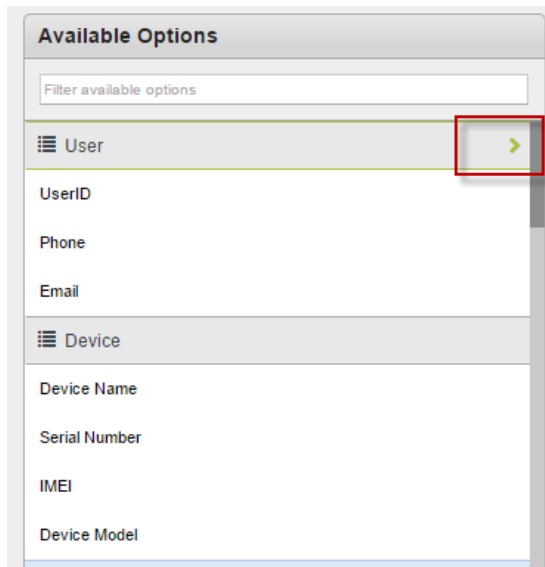
1. In Kony Management Suite Management console, click **Reports**. The Reports page appears.
2. Click **Compliance Actions**. The Compliance Actions Report page appears.

3. From the **Users** list, select **All** or **Specific**. If you select All, new fields do not appear. If you select Specific, new fields (Groups and Users) appear.
4. To create a Compliance Actions report for any specific group, enter the group name in the **Groups** field.
5. To create a Compliance Actions report for any specific user, enter the user name in the **Users** field.
6. From the **Compliance Violation** list, select the compliance violation type.
7. In the **From** field, select the compliance actions from date and time.
8. In the **To** field, select the compliance actions until date and time.
9. From the **Action** list, select the action.
10. From the **Platform** list, select the platforms for which you want the report.
11. Click **Next**. The Output Parameters page appears.

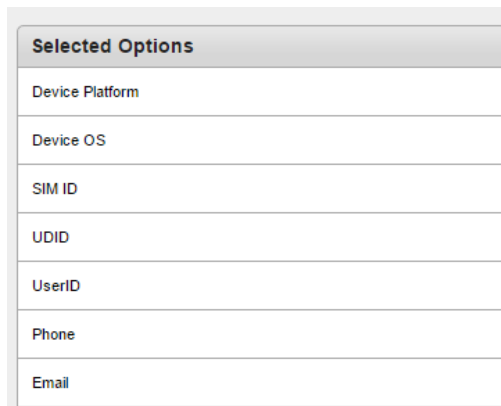
The Output parameters page displays all parameters in two columns: **Available Options** and **Selected Options**. In the Selected options column, some parameters are selected by default (Device Platform, Device OS, SIM ID, and UDID).

12. You can choose other parameters from the available options column. You can do that in two ways:
 - Select parameters group
 - Select individual parameter.

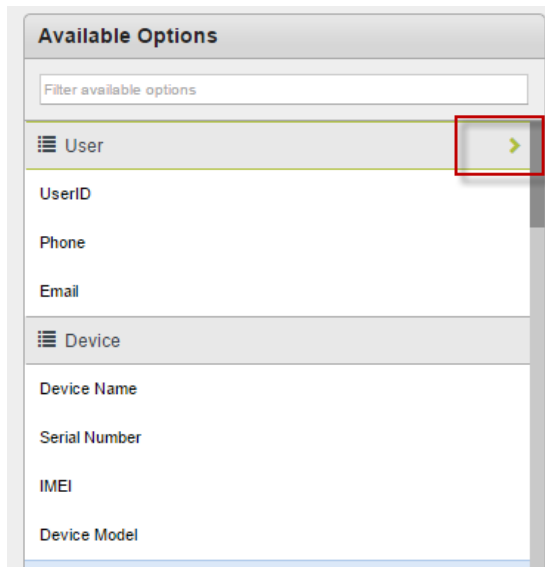
13. To select a parameters group, do the following:
 - a. Hover your mouse on the parameters group name. The select icon appears.



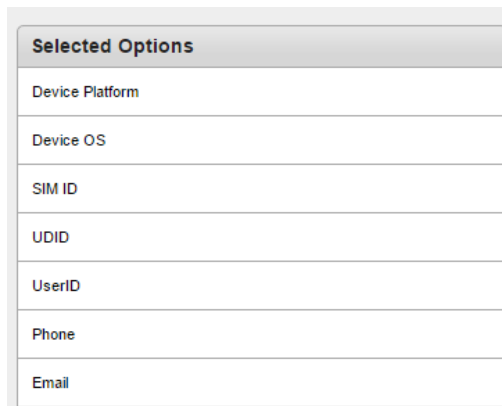
- b. Click the select icon. Selected parameters appear in the selected options column.



14. To select a parameters group, do the following:
- Hover your mouse on the parameters group name. The select icon appears.

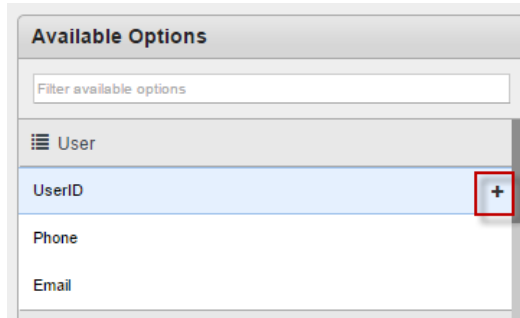


- Click the select icon. Selected parameters appear in the selected options column.



15. To select an individual parameter, do the following:

a. Hover your mouse over the parameter you want to select. A plus sign appears.



b. Click the plus sign. Selected parameter appears in the selected options column.

16. Click **Next**. The Report Generation page appears.

17. To view the report in a browser, select **Generate report in browser**.

18. To download the report, select **Download as**.

19. If you select Download as, select the file type from the **Download as** list. Options are CSV, PDF, XLS, and XLSX.

20. Click **Generate**. The report opens in a new browser or downloads in the chosen format.

13.2.5 Enterprise App Usage Report

The Enterprise App Usage report generates a report about app use on a device.

To create an App Usage report, follow these steps:

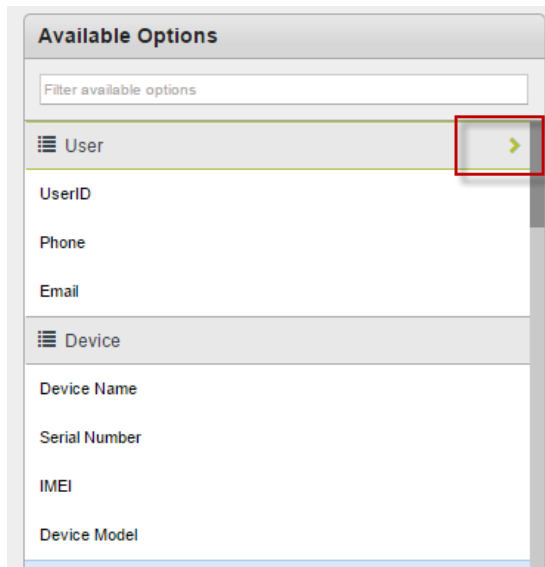
1. In Kony Management Suite Management console, click **Reports**. The Reports page appears.
2. Click **Enterprise App Usage Report**. The App Usage Report page appears.
3. From the **Target Users** list, select **All** or **Specific**. If you select All, new fields do not appear. If you select Specific, new fields (Groups and Users) appear.

4. To create an Enterprise App Usage report for any specific group, enter the group name in the **Groups** field.
5. To create an Enterprise App Usage report for a user, enter the user name in the **Users** field.
6. In the **Used From** field, select the from date and time.
7. In the **To** field, select the until date and time.
8. From the **Time Interval** list, select a time interval. Options are **Daily**, **Monthly**, and **Yearly**.
9. Click **Next**. The Output Parameters page appears.

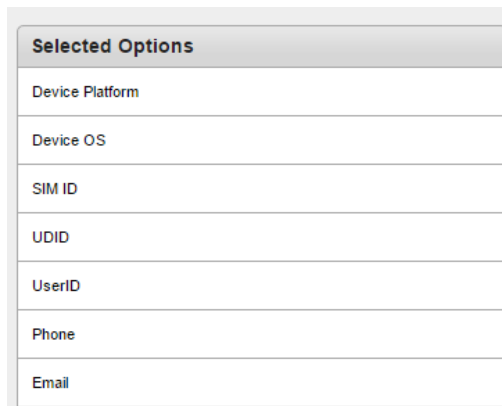
The Output parameters page displays all parameters in two columns: **Available Options** and **Selected Options**. In the Selected options column, some parameters are selected by default.

10. You can choose other parameters from the available options column. Select one of the following options:
 - Select parameters group
 - Select individual parameter.

11. To select a parameters group, do the following:
 - a. Hover your mouse on the parameters group name. The select icon appears.

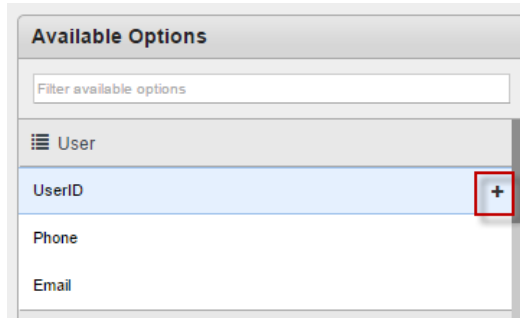


- b. Click the select icon. Selected parameters appear in the selected options column.



12. To select an individual parameter, do the following:

- a. Hover your mouse over the parameter you want to select. A plus sign appears.



- b. Click the plus sign. The selected parameter appears in the selected options column.

13. Click **Next**. The Report Generation page appears.

14. To view the report in a browser, select **Generate report in browser**.

15. To download the report, select **Download as**.

16. If you select Download as, select the file type from the **Download as** list. Options are CSV, PDF, XLS, and XLSX.

17. Click **Generate**. The report opens in a new browser or downloads in the chosen format.

13.2.6 Call Usage Report

The Call Usage report generates a report on call usage of a device in Kony Management Suite console.

To create a usage report, follow these steps:

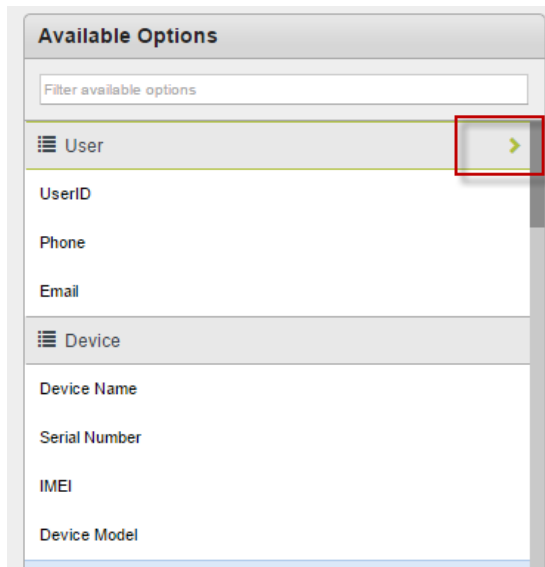
1. In Kony Management Suite Management console, click **Reports**. The Reports page appears.
2. Click **Call Usage Report**. The Call Usage Report page appears.

3. From the **Target Users** list, select **All** or **Specific**. If you select All, new fields do not appear. If you select Specific, new fields (Groups and Users) appear.
4. To create a call usage report for a group, enter the group name in the **Groups** field.
5. To create a call usage report for a user, enter the user name in the **Users** field.
6. In the **Used From** field, select the from date and time.
7. In the **To** field, select the until date and time.
8. From the **Time Interval** list, select a time interval. Options are **Daily**, **Monthly**, and **Yearly**.
9. Click **Next**. The Output Parameters page appears.

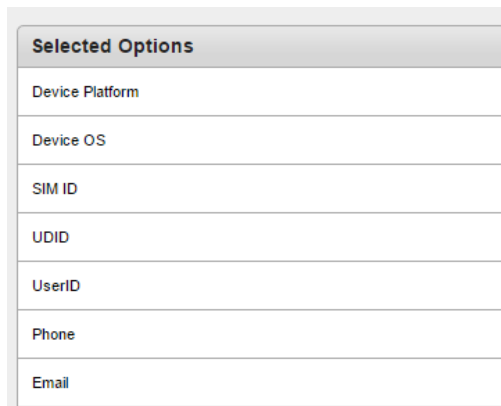
The Output parameters page displays all parameters in two columns: **Available Options**, and **Selected Options**. In the Selected options column, some parameters are selected by default.

10. You can choose other parameters from the available options column. Select one of the two options:
 - Select parameters group
 - Select individual parameter.

11. To select a parameters group, do the following:
 - a. Hover your mouse on the parameters group name. The select icon appears.

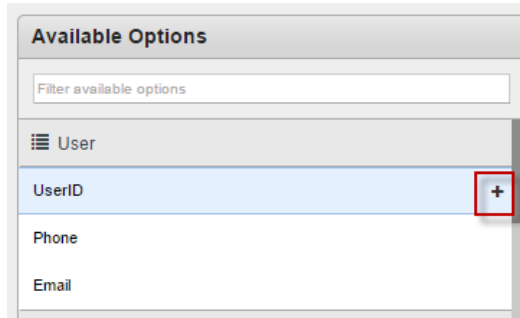


- b. Click the select icon. Selected parameters appear in the selected options column.



12. To select an individual parameter, do the following:

a. Hover your mouse over the parameter you want to select. A plus sign appears.



b. Click the plus sign. The selected parameter appears in the selected options column.

13. Click **Next**. The Report Generation page appears.

14. To view the report in a browser, select **Generate report in browser**.

15. To download the report, select **Download as**.

16. If you select Download as, select the file type from the **Download as** list. Options are CSV, PDF, XLS, and XLSX.

17. Click **Generate**. The report opens in a new browser or downloads in the chosen format.

13.2.7 SMS Usage Report

The SMS Usage report generates a report on SMS usage of any device in Kony Management Suite console.

To create an SMS usage report, follow these steps:

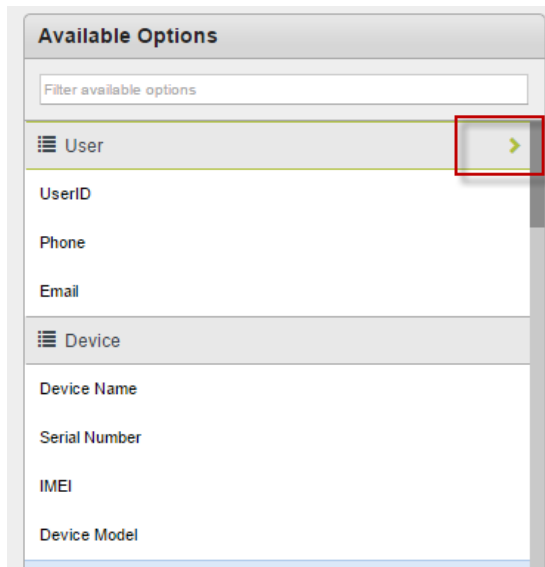
1. In Kony Management Suite Management console, click **Reports**. The Reports page appears.
2. Click **SMS Usage Report**. The SMS Usage Report page appears.

3. From the **Target Users** list, select **All** or **Specific**. If you select All, new fields do not appear. If you select Specific, new fields (Groups and Users) appear.
4. To create an SMS usage report, for any specific group, enter the group name in the **Groups** field.
5. To create an SMS usage report, for any specific user, enter the user name in the **Users** field.
6. In the **Used From** field, select the from date and time.
7. In the **To** field, select the until date and time.
8. From the **Time Interval** list, select a time interval. Options are Daily, Monthly, and Yearly.
9. Click **Next**. The Output Parameters page appears.

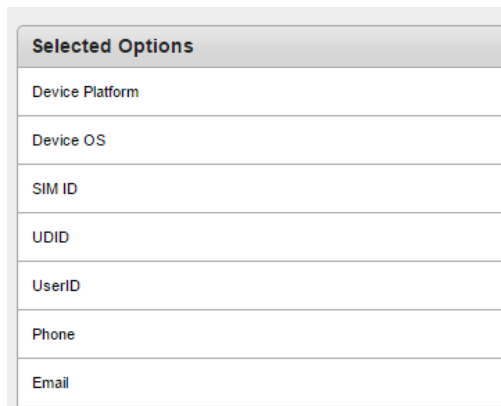
The Output parameters page displays all parameters in two columns: **Available Options** and **Selected Options**. In the Selected options column, some parameters are selected by default (Device Platform, Device OS, SIM ID, and UDID).

10. You can choose other parameters. from the available options column. Select one of the two options:
 - Select parameters group
 - Select individual parameter.

11. To select a parameters group, do the following:
 - a. Hover your mouse on the parameters group name. The select icon appears.

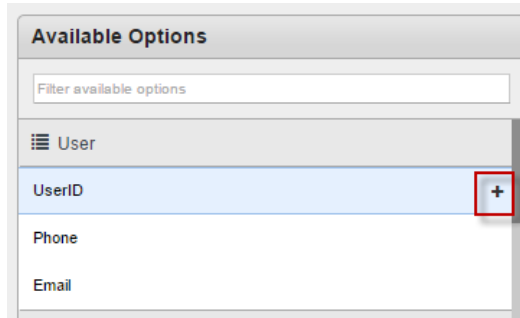


- b. Click the select icon. Selected parameters appear in the selected options column.



12. To select an individual parameter, do the following:

a. Hover your mouse over the parameter you want to select. A plus sign appears.



b. Click the plus sign. Selected parameter appears in the selected options column.

13. Click **Next**. The Report Generation page appears.

14. To view the report in a browser, select **Generate report in browser**.

15. To download the report, select **Download as**.

16. If you select Download as, select the file type from the **Download as** list. Options are CSV, PDF, XLS, and XLSX.

17. Click **Generate**. The report opens in a new browser or downloads in the chosen format.

13.2.8 Enterprise App Network Usage Report

The Enterprise App Network Usage report generates a report on compliance actions taken on targeted devices and violations, in Kony Management Suite console.

Important: For devices on Android OS 6.0 and above, the network usage report will not generate data.

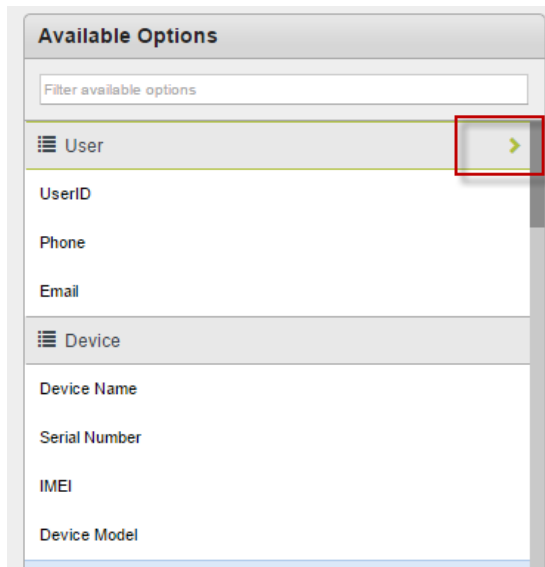
To create an Enterprise App Network Usage Actions report, follow these steps:

1. In Kony Management Suite Management console, click **Reports**. The Reports page appears.
2. Click **Enterprise App Network Usage**. The Enterprise App Network Usage Report page appears.
3. From the **Target Users** list, select **All** or **Specific**. If you select All, new fields do not appear. If you select Specific, new fields (Groups and Users) appear.
4. To create an App usage report for any specific group, enter the group name in the **Groups** field.
5. To create an App usage report, for any specific user, enter the user name in the **Users** field.
6. In the **Used From** field, select the from date and time.
7. In the **To** field, select the until date and time.
8. From the **Time Interval** list, select a time interval. Options are **Daily**, **Monthly**, and **Yearly**.
9. Click **Next**. The Output Parameters page appears.

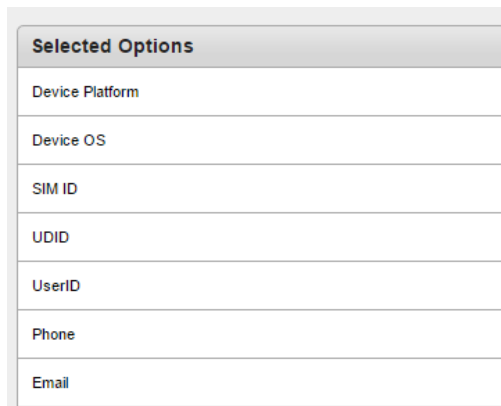
The Output parameters page displays all parameters in two columns: **Available Options** and **Selected Options**. In the Selected options column, some parameters are selected by default.

10. You can choose other parameters from the available options column. Select one of two options:
 - Select parameters group
 - Select individual parameter.

11. To select a parameters group, do the following:
 - a. Hover your mouse on the parameters group name. The select icon appears.

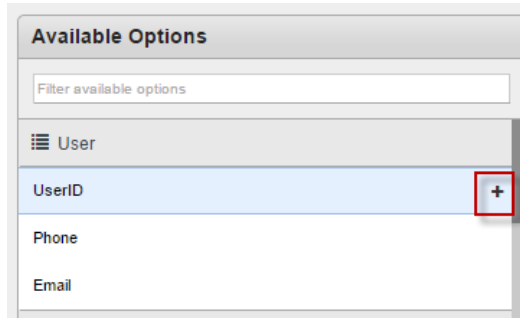


- b. Click the select icon. Selected parameters appear in the selected options column.



12. To select an individual parameter, do the following:

a. Hover your mouse over the parameter you want to select. A plus sign appears.



b. Click the plus sign. Selected parameter appears in the selected options column.

13. Click **Next**. The Report Generation page appears.

14. To view the report in a browser, select **Generate report in browser**.

15. To download the report, select **Download as**.

16. If you select Download as, select the file type from the **Download as** list. Options are CSV, PDF, XLS, and XLSX.

17. Click **Generate**. The report opens in a new browser or downloads in the chosen format.

Important: Network usage statistics limitation (on Android platform) on the higher-end devices from Marshmallow.

To support this feature on higher-end devices, you must manually enable the Usage Access permission from Settings > Security > App Usage Access > Enterprise Store for Launchpad.

13.2.9 User Device Report

The User Device Report generates a report on all users and their devices enrolled in Kony Management Suite console.

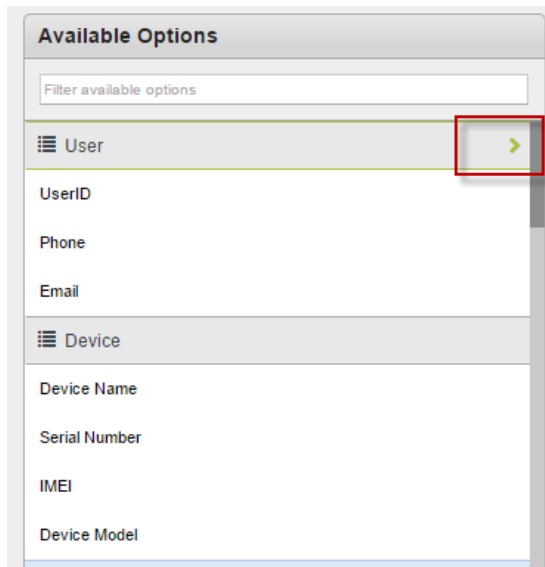
To create a User Device Report, follow these steps:

1. In Kony Management Suite Management console, click **Reports**. The Reports page appears.
2. Click **User Device Report**. The Device User Report page appears.
3. From the **Target Users** list, select **All** or **Specific**. If you select All, new fields do not appear. If you select Specific, new fields (Groups and Users) appear.
4. To create a Device User Report for any specific group, enter the group name in the **Groups** field.
5. To create a Device User Report, for any specific user, enter the user name in the **Users** field.
6. Click **Next**. The Output Parameters page appears.

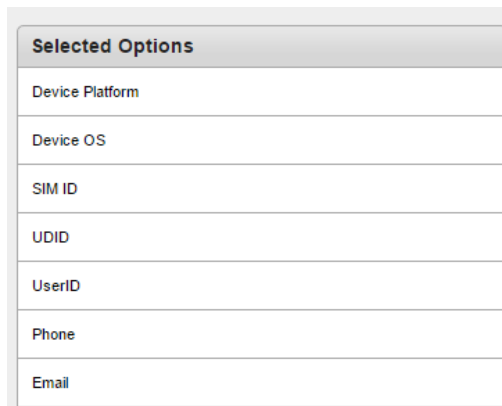
The Output Parameters page displays all parameters in two columns: **Available Options** and **Selected Options**. In the Selected Options column, some parameters are selected by default.

7. You can choose other parameters from the available options column. Select one of two options:
 - Select parameters group
 - Select individual parameter.

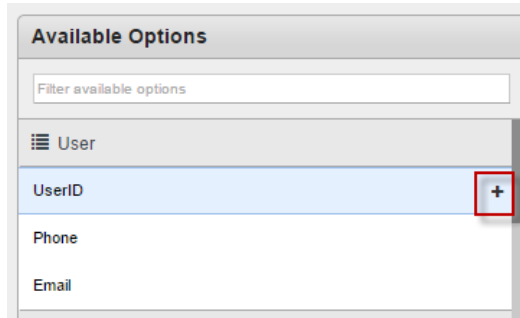
8. To select a parameters group, follow these steps:
 - a. Hover your mouse on the parameters group name. The select icon appears.



- b. Click the select icon. The selected parameters appear in the selected options column.



9. To select an individual parameter, do the following:
 - a. Hover your mouse over the parameter you want to select. A plus sign appears.



- b. Click the plus sign. Selected parameter appears in the selected options column.
10. Click **Next**. The Report Generation page appears.
11. To view the report in a browser, select **Generate report in browser**.
12. To download the report, select **Download as**.
13. If you select Download as, select the file type from the **Download as** list. Options are CSV, PDF, XLS, and XLSX.
14. Click **Generate**. The report opens in a new browser or downloads in the chosen format.

13.2.10 App Rating Report

The App Rating Report generates a report on all ratings for apps added in Kony Management Suite console.

To create an App Rating Report, follow these steps:

1. In Kony Management Suite Management console, click **Reports**. The Reports page appears.
2. Click **App Rating Report**. The App Rating Report page appears. with the Input Parameters tab open by default.

3. From the **App Type** list, select **All** or **Enterprise App**. If you select All, new fields do not appear. If you select other options, new fields may appear.
4. To create an app rating report for any app group, select the app group, for example Enterprise App. The App Name field appears.
5. Enter the app name in the **App Name** field.
6. From the **Platform** list, select **All** or any specific platform from the available list. If you select a specific platform, you will get a new field, **App Version**.
7. From the **App Version** list, select **All** or any specific app version from the available list.
8. Click **Next**. The Output Parameters page appears.

The Output Parameters page displays all parameters in two columns: **Available Options** and **Selected Options**. In the Selected Options column, some parameters are selected by default.

9. You can choose other parameters from the available options column. Select one of two options:
 - Select parameters group
 - Select individual parameter.
10. To select a parameters group, follow these steps:
 - a. Hover your mouse on the parameters group name. The select icon appears.
 - b. Click the select icon. The selected parameters appear in the selected options column.
11. To select an individual parameter, do the following:
 - a. Hover your mouse over the parameter you want to select. A plus sign appears.
 - b. Click the plus sign. Selected parameter appears in the selected options column.
12. Click **Next**. The Report Generation page appears.
13. To view the report in a browser, select **Generate report in browser**.
14. To download the report, select **Download as**.

15. If you select Download as, select the file type from the **Download as** list. Options are CSV, PDF, XLS, and XLSX.
16. Click **Generate**. The report opens in a new browser or downloads in the chosen format.

14. Management Error and Information Messages

The Management Error and Information Messages section displays error and information messages pertaining to the following sections:

- [Policy Messages](#)
- [Push Messages](#)
- [Store Messages](#)

The error messages provide a guideline to ensure that devices are compliant with policies. Each error message defines a scenario where a user can receive the specific error message. The error messages are displayed when a user uses a device in real-time. The error messages also enable a user admin to provide a suitable message to a device user to understand the real cause behind a technical issue. For example, a device user can receive an error message when trying to use an app beyond the defined geo-location to ensure corporate data safety. Similarly a device user can receive an error message to detect and report high risk and non-compliant devices.

14.1 Policy Messages

The following table displays the policy messages:

| Policy Messages | Cause/Scenarios |
|------------------------|--|
| App Idle Time Exceeded | The admin applies the Enterprise app policy for closing the app connection from server after not in use for a specific time duration set in the policy. The user receives the policy error message, if tries to access the application after a set duration. |
| App Locked | The admin applies the Enterprise app policy of App Lock to restrict the user to use the app. When launched, the device displays the policy error message and closes the app automatically. |

| Policy Messages | Cause/Scenarios |
|---|--|
| App Expired | The admin applies the Enterprise app policy to set the enterprise app validity for a specific date/time. The user receives the policy error message- App Expired, if the user tries to access the application after the app validity period. |
| Cannot use the app on business off day | The admin applies the Enterprise app policy for restricting the user to use the app only on specific days. When a user tries to use the app after or before the allowed day, the device displays the message and close the app automatically. |
| Business Hour Expired | The admin applies the Enterprise app policy for restricting the user to use the app only in a specific time frame. When a user tries to use the app after or before the allowed time frame, the device displays the message and close the app automatically. |
| App running outside App region | The admin applies the Enterprise app policy for restricting the user to use the app only in a specific geolocation. When a user tries to use the app outside the allowed geolocation area, the device displays this message and close the app automatically. |
| The app must be launched from the Enterprise Store only | The admin selects the option Allow Direct Launch flag as No while creating an app. When a user tries to launch the app from the springboard or outside the Launchpad, the device displays this message. |
| The app can only be launched from within Enterprise Store while device is offline | The admin has applied a policy where: <ul style="list-style-type: none"> - Allow Offline Access is selected as Yes - and while creating an app - Enabled the flag Allow Direct Launch as No - and If the device is in offline mode and a user tries to access the app. The device displays this message. |

| Policy Messages | Cause/Scenarios |
|---|--|
| App is not allowed to be used in offline mode. | The admin has applied the policy Allow Offline Access as No . When a device is offline and a user tries to access the app, the device displays this Policy message. |
| App must be launched in online mode at least once. Enterprise store is not reachable. Unable to fetch policy. Please try again later. | The device user has installed any app from the Enterprise Store, but not yet launched the app online. When a user tries to use the app while the server is in offline mode, the app cannot receive the policy from the server. The device displays this message. |
| No network connectivity on device. App must be launched in online mode at least once to fetch the app usage policy from server. | The device user has installed any app from the Enterprise Store, but not yet launched the app online. When a user tries to use the app while the device is in offline mode, the app cannot receive the policy from the server. The device displays this message. |
| This app requires iOS 4.0 or above | The OS version running on an iOS device is below 4.0. The device prompts the message to a user as per EMM support. |
| Application source is not verified and it may be malicious. Uninstall current Application and download the latest app version from the Enterprise store | The error appears if the finger-print of signing certificate does not match for the child app and Launchpad. It indicates that the child app is tampered in between and signed with a different certificate. |
| Policy violation. Camera Access not allowed | The admin applies the Enterprise app policy from the App Usage section to restrict the user from using the camera through the app. When a user tries to use the app's camera, the device displays the message. |

| Policy Messages | Cause/Scenarios |
|---|---|
| Policy violation. Cut,Copy and Paste operations not allowed | The admin applies the Enterprise app policy from the App Usage section to restrict the copy, cut, and paste operation on the app content. When a user tries to perform any such operation on app content, the device displays the message. |
| Policy violation. Document sharing not allowed | The admin applies the Enterprise app policy from the App Usage section to restrict the user from performing any sharing operation on the app content shown. When a user tries to perform such operation on the app content, the device displays the warning message. |
| Policy violation. Email to this address is not allowed | The admin applies the Enterprise app policy from the Phone Feature section for restricting the user to send the mail on specific mail ids through app. When a user tries to send any mail on restricted mail ids, the device displays the warning message. Here the admin can provide the list of restricted mail ids by comma separated values in a list. |
| Policy violation. Email Access not allowed | The admin applies the Enterprise app policy from the Phone Feature section for restricting the user to send the mail on any mail ids through the app. When a user tries to send a mail on restricted mail ids, the device displays the warning message. Here the admin can provide the list of all restricted mail ids name by comma separated values in a list. |
| Enterprise Store must be installed on device, otherwise you cannot launch any enterprise apps | This error appears if the Enterprise Store is deleted from the device and trying to launch the app installed through EMM. |
| Policy violation. External read not allowed | The admin applies the Enterprise app policy from the Storage section for restricting the app to read the data from external storage devices such as an SD card .If the app tries to read the data from such any external source, the device displays the warning message. |

| Policy Messages | Cause/Scenarios |
|--|--|
| Policy violation. External write not allowed | The admin applies the Enterprise app policy from the Storage section for restricting the app to write the data to external storage devices such as an SD card. If the app tries to write the data from such any external storage, the device displays the warning message. |
| Unable to retrieve location. Enable location services and relaunch the app. | This message appears on an iOS device if the location services is not ON for the Enterprise Store. |
| Mocking locations is not allowed. Disable this option in the device settings | The admin set the value in Kony Management console on the Device setting page >Tracking Settings > Allow Mock Location as No . But still on a device the setting is enabled for mocking the location under the Developer option. Thus the device prompts the user with an error message to disable the Mock Location on a device. |
| Policy violation. Network Access not allowed for the currently active Wi-Fi | The admin applies the Enterprise app policy from the Network section for restricting a user to use a few specific WI-Fi for an app. When a user tries to open or launch the app using restricted WI-Fi, the system displays the warning message. Here the admin can provide a list of restricted WI-Fi IDs by comma separated values in a list. |
| Policy violation. Network Access through wi-fi not allowed | The admin applies the Enterprise app policy from the Network section for restricting the user to use any Wi-Fi for an app. When a user tries to open or launch the app using restricted Wi-Fi, the system displays the warning message. Here the admin can set regular expression such as "*" for blocking the user to use the app with any Wi-Fi SSIDs. |
| Policy violation. Network Access not allowed | The admin applies the Enterprise app policy from the Network section for restricting the user to make a network call through an app. When a user tries to open or perform any action on app which makes any network call, the device displays the warning message. |

| Policy Messages | Cause/Scenarios |
|--|---|
| Policy verification failed. Maybe an attempt to spoof the network. | If the policy is tempered in between the calls, it is determined through a mechanism. Thus the device displays the error message. |
| Cannot Access Messages You must connect to a Wi-Fi or mobile data network to access Messages | At an Enterprise Store, the messages are available as online content. A device can access the message list online through network connectivity to fetch a list of messages from the server. If the device goes offline due to lack of network connectivity, the user is prompted with the warning message: Cannot access messages. You must connect to a Wi-Fi or mobile data network to access messages. |
| You have exceeded your authentication failure limit. You may no longer use Enterprise Store offline. Try to login while online | The admin has configured a value for the option Maximum Failed Attempts Offline login on the Application Settings page > Usage Settings tab. When a user crosses the limit of offline attempts, the user is asked to login online to access the Enterprise Store again (in offline mode). If the user tries to login offline again, the device displays the warning message. |
| Policy violation. Phone call to this number is not allowed | The admin applies the Enterprise app policy from the Phone features to restrict a user from making a call on specific mobile number through an app. When a user tries to call on the restricted number using an app, the device displays the warning message. Here the admin can provide the list of restricted mobile numbers by comma separated values. |
| Policy violation. Phone Access not allowed | The admin applies the Enterprise app policy from the Phone features to restrict a user from making a call on specific mobile number through an app. When a user tries to call on restricted mobile number using an app, the device displays the warning message. Here the admin can set the regular expression to restrict the calling on a mobile number by putting "*" in the given list. |

| Policy Messages | Cause/Scenarios |
|--|---|
| Policy mismatch detected. Now the app must be launched online to fetch the new policy. | If the policy is tempered in between the calls. It calculates through hashing mechanism and prompts the user for the action.(Need more clarification from SME) |
| Client certificate is revoked | This message is shown if the SCEP certificate is revoked from the SCEP server. |
| Session has expired. Login through the Enterprise Store. | The admin applies the Enterprise app policy from the App Usage section. The policy pertains to the expired session of logged-in users where a user crosses the set idle time out duration on the app, This policy expires the Enterprise Store session only when Allow Direct Launch is turned off under App Details for an app. In this scenario, a user will be asked to re-login to the Enterprise Store to access the app. |
| Policy violation. SMS to this number is not allowed | The admin applies the Enterprise app policy from network section to restrict a user to access any specific domain through an app. When a user tries to open the URL using the app, the device displays the warning message. |
| Policy violation. Specified domain not allowed | If admin applies an enterprise app policy from network section for restricting the user to access any specific domain through an app and User tries to open that URL using an app having this restriction applied by admin then it prompt with message. |
| Policy violation. SMS access not allowed | The admin applies the Enterprise app policy from Phone features to restrict a user to send messages to any number through an app. When a user tries to send the SMS using an app, the device displays the warning message. Here the admin can set the regular expression to restrict the messaging on any mobile number no by putting "*" in the given list. |

14.2 Push Messages

The following table displays the push messages:

| Push Messages | Scenarios |
|--|---|
| <p>Your device has been blocked by EMM Admin. You will be logged out.</p> | <p>The admin performs the Block device operation from Device Details for the MAM mode device. The Block device operation restricts the access to the Enterprise Store resources. When a user tries to access the enterprise resources, the user is notified with a push message.</p> |
| <p>Your device has been deactivated by EMM Admin. You will be logged out.</p> | <p>The admin performs the device Wipe operation and selects the wipe type as Deactivate from the device details for the EMM mode devices. The operation restricts the access to Enterprise Store and deletes all Enterprise data. As an action the device enrolment is also removed and push message sent to notify the user device.</p> |
| <p>Your account has been deactivated by EMM Admin. You will be logged out.</p> | <p>The admin performs deactivate or delete user operation from the Users list page. The action to deactivate or delete a user for the enrolled devices restricts access to the Enterprise store, and the user is logged out immediately from the store. A push message is sent to notify the user device.</p> |
| <p>This device is Deactivated. You will not have access to any enterprise resources. Contact your IT Admin in case you have any queries.</p> | <p>The admin performs the user deletion or deactivate user operation from the Users list page. The action to delete or deactivate a user for the enrolled user devices (deactivate) restricts the access to Enterprise Store. The action also removes the device enrolment. A push message is sent to notify the user device.</p> |
| <p>This device was reported as Lost. Due to which it is wiped. You will not have access to any enterprise resources. Contact your IT Admin in case you have any queries.</p> | <p>The admin performs Complete Wipe operation for the Corporate or Shared ownership devices which are in EMM mode. The admin selects the wipe type as Device Lost. The action performs the complete wipe operation by erasing all device data along with device enrolment. A push notification is sent to the user device.</p> |

| Push Messages | Scenarios |
|--|--|
| <p>Your device is purged by EMM Admin. You will be logged out.</p> | <p>The admin performs the device Purge operation to remove the device enrollment from Kony EMM. The purge operation is for those devices that are wiped, but not yet updated to serve because of network issues. The action performs Enterprise wipe, changes the device - status as control removed, and delete the device enrollment. Now the device can be re-enrolled again. A push message is sent to notify the user.</p> |
| <p>This device is Resumed. You will have access to enterprise resources. Contact your IT Admin in case you have any queries.</p> | <p>The admin performs the Resume Device operation for any suspended device from Device Details to enable the access to Enterprise store. The action changes the device enrollment state to Enrolled. Now, the device can access all Enterprise resources again that got removed earlier as an action of Suspended wipe. A push message is sent to notify the user.</p> |
| <p>This device is Retired. You will not have access to any enterprise resources. Contact your IT Admin in case you have any queries.</p> | <p>The admin performs the Retired Wipe operation for the EMM mode devices from the Device Details page. Based on the selected Retired Wipe operation as Enterprise Wipe or Complete wipe, the EMM server takes the appropriate action. A push message is sent to notify the user.</p> |
| <p>This device is Suspended. You will not have access to any enterprise resources. Contact your IT Admin in case you have any queries.</p> | <p>The admin performs the Suspended Wipe operation to temporarily block a user from accessing the Enterprise Store and removing the Enterprise data for any compliance violation. The action maintains the device enrollment as active, but a user cannot access the store unless an admin resumes the device. A push message is sent to notify the user.</p> |
| <p>Your device has been sent the Block corporate email command. In case you have any queries, contact your IT Admin.</p> | <p>The admin performs the Block Email operation from the Device Details page. The action prevents a user from accessing the Enterprise Email account. A push message is sent to notify the user.</p> |

| Push Messages | Scenarios |
|---|---|
| <p>Email has been Unblocked on this device. You will now have access to email again. Contact your IT Admin in case you have any queries.</p> | <p>The admin performs the Unblock Email operation from the Device Details page. The action enables a user to access the Enterprise Email account that was blocked for any compliance violation. A push message is sent to notify the user.</p> |
| <p>Dear \${userName}, You have successfully enrolled your \${deviceModel} device. In case of any queries, please contact your IT Admin.</p> | <p>A user device is enrolled with the EMM server. A push notification to confirm device enrollment is sent to the user.</p> |
| <p>Dear \${userName}, You have successfully enrolled your \${deviceModel} device with device code \${deviceCode}. In case of any queries, please contact your IT Admin.</p> | <p>A user enrolls windows 8.0 device with the EMM server. A push notification to confirm device enrollment based on the device code is sent to the user.</p> |
| <p>Your Mail+ is Configured. Accept to start using emails.</p> | <p>The admin pushes the Email Configuration of "Mail +" for devices. A user configures this email client and sync with mail account. A push notification to confirm the email configuration is sent to the user.</p> |
| <p>You are required to Install \${appName} on this device. Check your pending actions to do the same.</p> | <p>The admin pushes any required MDM app policy for devices. A push notification is sent to notify the user. The push notification states that the user needs to install the app to check pending actions.</p> |

| Push Messages | Scenarios |
|--|--|
| <p>Your device enrollment mode has been changed to <code>#{enrollmode}</code> by EMM Admin. Please login to continue. In case of any queries, Contact your IT Admin.</p> | <p>The admin changes the Enrollment mode of the device from EMM to MAM or MAM to EMM. A push notification is sent to notify the user. The notification states that the enrollment mode is changed by the EMM Admin. The action asks a user to login to Launchpad and change the mode to continue with it. The action may restrict the user to login for a while when wipe is in progress (removing the resources not allowed for that mode).</p> |
| <p>The folder <code>#{foldername}</code> is now shared with you by <code>#{sharedbyname}</code>. You now have access to all its contents.</p> | <p>The EMM user shares a folder available in the user space to an EMM user. A push notification is sent to the user. The notifications states that the user can access all contents of the shared folder according to the content policy applied.</p> |
| <p>The folder <code>#{foldername}</code> is no longer shared with you by <code>#{sharedbyname}</code>.</p> | <p>The EMM user removes sharing of a folder with a user. A push notification is sent to the device user stating that the specific folder is no longer shared.</p> |
| <p>The file <code>#{filename}</code> is shared with you by <code>#{sharedbyname}</code>. You now have access to read the file.</p> | <p>The EMM user removes sharing of any file with any user. A push notification is sent to the device user stating that the specific file is no longer shared.</p> |
| <p>The file <code>#{filename}</code> is no longer shared with you by <code>#{sharedbyname}</code>.</p> | <p>The EMM user removes sharing of any file with any user. A push notification is sent to the device user stating that the specific file is no longer shared.</p> |
| <p>The folder <code>#{foldername}</code> is now available to you with all its contents.</p> | <p>The EMM admin shares any folder with an EMM user. A push notification is sent to the user. The notification states that the specific folder is shared by the EMM admin and the user can access all content according to the content policy applied.</p> |

| Push Messages | Scenarios |
|--|--|
| The folder <code>{{foldername}}</code> is no longer available to you. | The EMM admin removes sharing of any folder with any EMM user. A push notification is sent to the user stating that the specific folder is no longer available from EMM admin. |
| Content available to you has been updated. | The EMM admin updates any content of the targeted folder to any EMM user. A push notification is sent to the user stating that the available content is updated. |
| The file <code>{{filename}}</code> has an updated version <code>{{versionnum}}</code> available. You can sync the same to your device as required. | The EMM admin updates any file available to any user. A push notification is sent to the user. The notification states that the new updated version file name is available and the user can sync the content to receive the new changes. |
| App <code>{{appname}}</code> is available on the Enterprise Store. | The notification is sent to the device user when the EMM admin targets an app. The push notification notifies the user that the specific AppName is available on the Enterprise store. |
| New Apps are available on the Enterprise Store. | The notification is sent to a device user when the user is added to a new group to which several apps are targeted. Thus the push message is sent to a user in case of group or user re-targeting. |
| New Mandatory Apps are required on your device. | The notification is sent to a device user when several mandatory apps become available. The user is added to a new group to which these apps are targeted. Thus the push message is sent to a user in case of group or user re-targeting. |
| Mandatory App <code>{{appname}}</code> is required by your device. | The EMM admin targets any mandatory app to a user that must be installed on the device. If the user cancels or due to network related issue, the app installation is not complete, the push notification prompts again and again to a device user to install the app on a device. The device user gets this notification after refreshing the My Apps Page in the Enterprise Store. |

| Push Messages | Scenarios |
|---|--|
| An upgrade for Enterprise Store is available on your device. | The admin upgrades the Enterprise Store explicitly or wrapping gets initiated implicitly the Enterprise Store. A push notification is sent to the device user stating that the Enterprise Store upgrade is available. |
| All App data related to all Enterprise Apps will be cleaned up. | The EMM admin performs Remove App Data operation from the Device Details page to delete all enterprise app data. A push notification is sent to the device user stating that all Enterprise app data will be cleaned up. |
| Upgrade for \${appname} is no longer available. | The EMM admin has upgraded an existing app from version x.0 to the higher version, such as x.1 in the EMM console. The new version of the app is available on a user's device. The device user does not install the app on the device and later the EMM admin un-publishes the upgraded version of the app. In this scenario, a push notification is sent to the device user stating that the upgrade is no longer available for the specific app. |
| Several app upgrades are now revoked and no longer available. | <p>The current scenario:</p> <ul style="list-style-type: none"> - A notification is sent to the device user when several upgrades to an app are revoked by the user. - The user is removed from an existing group to which the apps are targeted. <p>But still the user has access to a lower version of the app .This state happens when a group or a user re-targeting occurs.</p> |
| Your access for several apps has been revoked and they shall no longer be available to you. | The push notification is sent to the device user when several apps get revoked from the user. As user is removed from an existing group to which these apps had been targeted. Thus the push notification is sent to a user in a situation of group or user re-targeting. |
| Your access for \${appname} has been revoked. | The EMM admin un-publishes an app from the EMM console and that app is already installed on a user's device. A push notification is sent to the user stating that the specific app is no longer available. |

| Push Messages | Scenarios |
|--|---|
| An upgrade for <code>{appname}</code> (<code>{appversion}</code>) is now available. | The EMM admin upgrades any existing app with version x.0 to any higher version such as x.2. A push notification is sent to the device user stating that the new version of the app is available. |
| Upgrades for several apps are now available. Go through Enterprise Store to install them. | The notification is sent to a device user when the user is added to a new group where several upgrades to apps are available. Thus the push notification is sent to a user in a situation of the group or a user re-targeting. |
| Mandatory upgrades of several apps are required on your device. Download through Enterprise Store as required. | The notification is sent to a device user when the user is added to a new group where several mandatory upgrades to apps are available. Thus the push notification is sent to a user in a situation of group or user re-targeting. |
| A mandatory upgrade for <code>{appname}</code> (<code>{appversion}</code>) is required on your device. | The EMM admin upgrades any mandatory app with version x.0 to any higher version such as x.1. A push notification is sent to the device user stating that the mandatory upgrade of the app is available such as <code><app name> with <app version></code> . |

14.3 Store Messages

The following table displays the store messages:

| Store Messages | Scenarios |
|----------------|--|
| Access denied | This is a generic message shown if the user does not have the permission to access the Enterprise Store. |

| Store Messages | Scenarios |
|--|--|
| Cannot connect to Active Directory | The error appears when a user tries to login to Enterprise Store and any ADS exception occurs while authenticating with the AD user. |
| Certificate cannot be downloaded. Contact your administrator | The error appears for the Windows platform when a user tries to download the AETX certificate from the server and does not find the certificate at the specified location. |
| Password should contain only alphabets. | The settings is provided on the Application Settings > Usage Settings page under the section Local EMM User Password Settings . If the password is not provided as per the rules, the system asks the user to reset the password. As per the rules, while resetting the password the current password should contain only alphabets. |
| Password should contain only Alphabets and digits. | The settings is provided on the Application Settings > Usage Settings page under the section Local EMM User Password Settings . If the password is not provided as per the rules, the system asks the user to reset the password. As per the rules, while resetting the password the current password should contain only alphabets and digits. |
| Error occurred while performing the operation, Contact your administrator | This is a generic message shown if any process is interrupted before completion because of any network or environment issue. |
| Invalid User attribute value received from OAuth2 server. | The system displays the error if an invalid user attribute value is received from OAuth2 server or OAuth2 provider. The response attribute '{0}' value is empty or null in the user profile. |

| Store Messages | Scenarios |
|--|--|
| Authentication failed. | The system displays the error if an internal error occurred while trying to authenticate the user with OAuth2 provider. As the user authentication is not completed, the error appears for the authentication failure. |
| Enrollment configuration error. EMM Admin must update server settings. | The system displays the error if the authentication setting is configured with OAuth2 by the EMM admin and server returns a null value for the OAuth2 configuration. |
| The User does not exist. Contact your EMM admin. | The system displays the error after the successful user authentication with the OAuth2 server. If the user does not exist in the EMM server, the device displays the error message. |
| Failed to get profile endpoint | The OAuth2 authentication tries to get the profile endpoint for the requested user profile data. If the system is unable to find the profile end point, the error message is displayed. |
| Invalid profile endpoint response (json parse error). | The OAuth2 authentication tries to get the profile endpoint for the requested user profile data. If the returned profile end point is not a valid JSON response, the device displays the error message. |
| Failed to get profile endpoint (json read error). | The OAuth2 authentication tries to get the profile endpoint for the requested user profile data. If the returned profile end point is not a valid JSON response, the device displays the error message. |
| The User is inactive. | The EMM admin has deactivated a user in the EMM server and the user tries to login on Launchpad. In this scenario, the device displays the error message. |

| Store Messages | Scenarios |
|--|---|
| The User attributes exchange failed. | The OpenID2 provider response attributes does not match with the requested attributes .This scenario occurs if the attribute list configured by the EMM admin does not match with the list returned by OpenID 2.0 provider while getting the user details. In this scenario, the device displays the error message. |
| Invalid User attribute value received from OpenID 2 server. | The device displays the error if the OpenID2 provider response attribute '{}' value is empty or null. |
| Authentication failed. | An internal error occurs while trying to authenticate the user with OpenID2 provider. As the authentication is not complete, the device displays the error for the authentication failure. |
| Enrollment configuration error. The EMM admin must update the server settings. | <p>The system displays the following error messages, if the authentication settings is configured with OpenID2 for the following scenarios:</p> <ol style="list-style-type: none"> 1. On Windows platform, while downloading Launchpad, the system checks for the company name provided on the Device Setting page (in the EMM console). If the company name is not provided, the system does not allow to proceed with Launchpad download. In this scenario, the device displays the error message for the improper settings. 2. On the Launchpad download page, the system tries to get the OpenID2 redirect URL for authentication for all platforms. If the redirect URL for OpenID2 server is blank, the device displays the error message for improper settings configuration at EMM server. |
| Unable to connect to authentication server. Try again. | The device displays the error message if the authentication settings is configured for OpenID2 and if any exception occurs while generating OpenID 2.0 auth redirect URL. |

| Store Messages | Scenarios |
|--|---|
| Unable to process claimed identity {arg0} | The authentication settings is configured with OpenID2 . If the OpenID 2.0 Provider identifier configured by EMM admin fails to consume while generating OpenID2 redirect URL, the device displays the error message. |
| Your device platform is not supported. | The authentication settings is configured with OpenID2 . While downloading Launchpad, if the platform authentication fails, the device displays the error message for un-supported platform. |
| User does not exist. Contact your EMM admin. | The authentication with the OpenID2 server for a user is successful. The system looks for the corresponding user in the EMM server, and if the user does not exist, the device displays the error message. |
| User is inactive. | The EMM admin has deactivated a user in the EMM server and if the user tries to login on Launchpad, the device displays the error message. |
| Your device has been blocked by EMM Admin. You will be logged out. | The EMM Admin has performed device Block operation to restrict the device user to access the Enterprise Store. Thus when a user tries to access the Enterprise Store, the device displays the error message. |
| Incorrect Captcha. Try again | The user does not enter the valid captcha as displayed on the Enterprise Store login page. The option of captcha is asked only if the admin has enabled the setting on the Application Settings page under the Usage Settings tab for Online Login - Web and Enterprise Store section > Require Captcha as Yes. |
| An error occurred in invoking the command | While invoking the MDM commands for specific device if any MDM exception occurs, the device displays the error message. |

| Store Messages | Scenarios |
|--|--|
| An error occurred while fetching the command name | The system sends the command to a device to get the command name (for the given command Id) using the command map. If the map does not exist with given command Id and name, the device displays the error message. |
| Contact your administrator | The error message appears on multiple places but this case is for the Windows device as per store messages. If the device user does not have permission or any exception occurred while downloading the container for Windows platform. |
| Your device has been deactivated by EMM Admin. You will be logged out. | The EMM admin performs the device Wipe operation for restricting access to the Enterprise Store. The system displays the error message when the user is logged out from the Launchpad. |
| Device {arg0} is already enrolled with another user {arg1}. | The user tries to enroll a device whose enrollment is active with other user. In this scenario, re-enrollment of the device is not permitted with a new user unless previous user enrollment is not removed. For a new enrollment, the EMM admin either perform Device Purge operation (If in EMM mode)/ Device Block and Delete operation (If in MAM mode) from the Device list page. The device user may also try by removing the MDM profile if the device was enrolled in the EMM Mode earlier. |
| Device was already enrolled | When a user login to Launchpad and finds that the device is already enrolled with different user. In this scenario, the device displays the error message. |
| Device cannot be enrolled | The device enrolled state is LOST , RETIRED , and ALREADY ENROLLED . If the device is enrolled again the device displays the error message. |
| Device was deactivated | The device state is deactivated and added to enrollment denied list. So when a user tries to re-enroll the device, the device displays the error message. |

| Store Messages | Scenarios |
|---|--|
| Device enrollment denied. Contact your administrator | The EMM admin performs device wipe operation and selects the option Allow Future Enrollment as No . If a user still tries to enroll the device, the device displays the error message. |
| Device was lost | The EMM admin performs device wipe operation and selects the option Allow Future Enrollment as No. The current device state is Device Lost. If a user still tries to enroll the device with device id, the device displays the error message. |
| You are not allowed to register with this device. This device is already enrolled with another user. Contact your administrator | A user tries to enroll a Windows device. During device enrollment, the user checks the device auth- code for the device current state. If the device is enrolled with another user, the system displays the error message. |
| Device was retired | A user tries to enroll a device. During device enrollment, the user checks for the device current state. If the device current state is Retired , the device displays the error message. |
| Your device is no longer enrolled with EMM. Enroll your device again or contact your administrator in case of further queries. | A device user tries to login in the EMM mode. If a user gets the device enrolment state from the server as CANT LOGIN, the user device is not allowed to login. In this scenario, the device displays the error message for the new enrolment. |

| Store Messages | Scenarios |
|---|--|
| <p>This device is blocked for you and you cannot access your apps on the same. Contact your EMM Admin for more information.</p> | <p>The error appears for the MAM mode devices while login to the Enterprise store, if the EMM admin has blocked the device.</p> |
| <p>Your access to corporate resources is suspended. Contact your administrator in case of any further queries.</p> | <p>A user tries to login to the Enterprise Store through the EMM mode device. If the EMM admin has suspended the device for a temporary period to restrict the access to the Enterprise Store, the device displays the error message.</p> |
| <p>There are no users with the given email id. Provide a valid email id.</p> | <p>On Windows platform, a device user tries to login or download the EMM agent. In this scenario, a user is verified with the given Email Id in the EMM server. If the user does not exist with given email id, the device displays the error message.</p> |

| Store Messages | Scenarios |
|--|--|
| Device enrollment failed | <p>The error message can appear at multiple places during enrollment:</p> <ol style="list-style-type: none"> 1. This can be seen for all platforms if an exception occurred while parsing the enrollment request data. 2. While enrolling an Android device the MDM enrollment response data is invalid. It can happen because of any exception occurred while enrolling the device. In this scenario, the system cannot enroll the device and displays the error message. 3. The SCEP for android is set as YES in the Usage Settings and the Public key value is incorrect/missing in the enrollment request. In this scenario, the system cannot enroll the device and displays the error message. 4. During Windows phone enrollment in MAM only mode, the device registration process is not complete due to some exception. In this scenario, the system cannot enroll the device and displays the error message |
| Device enrollment failed. Try again or contact your administrator | <p>The error appears during a device enrollment, if the device does not have a valid enrollment request.</p> |
| Wipe has been initiated for this device. You are not permitted to login until it is completed. | <p>A user tries to login to the Enterprise Store and the device Wipe command is still in-progress mode. The situation can occur in the following scenarios:</p> <ul style="list-style-type: none"> - The EMM admin can initiate wipe for any wrong failed attempts <p>or</p> <ul style="list-style-type: none"> - The User device mode changes from EMM to MAM (for iOS and Windows). <p>In this scenario, the system displays the error message.</p> |
| IOException writing file to output stream | <p>The error message is displayed in the following scenarios:</p> <ol style="list-style-type: none"> 1. For Windows platform, if any exception occurs while downloading the aetx certificate from docroot to the Windows device. 2. For iOS platform if any exception occurs while downloading the MDM attribute profile from docroot to the device during enrollment. 3. For an iOS device for POC enrollment as well if any exception occurs while downloading the device attribute profile to a device for enrollment. |

| Store Messages | Scenarios |
|--|---|
| Internal server error. Contact your administrator | In the POC enrollment process if any exception occurs while processing the request for a device enrollment (for data reading operation), the device displays the error message. |
| Invalid Device Object. | The error message is displayed in the following scenarios: <ol style="list-style-type: none"> 1. During enrollment request if the device information is empty or null. 2. While validating the device login, the device information data is null. 3. During the device pre-enrollment, checking for the device current state and enrollment request flag. It is found that the device information data is null. |
| Invalid Device id | The error message is displayed in the following scenarios: <ol style="list-style-type: none"> 1. While sending the heartbeat the device id value is null or while getting the device id from request parameter, any exception occurs. 2. While getting the device logs call, if the device ID value is null or fails to read from the request. |
| Invalid enrollment URL. Check the URL for proper spelling and capitalization | In the POC enrollment mode, processing the enrollment request for a device. Due to an invalid enrollment request id, the device displays the error message. |
| INVALID_INPUT | On Android platform, if the EMM sever receives an invalid command action request from a device, the device displays the error message. |
| Invalid kony device id | While sending the MDM commands for a Kony device ID, if the device object information is NULL, the device displays the error message. |

| Store Messages | Scenarios |
|---|--|
| One or more input params are not in the valid format. | The scenario pertains to validating the enrollment request parameters. While reading a device object, if any JSON mapping exception or JSON parse exception occurs, the device displays the error message. |
| Invalid phone number | While reading the phone number parameter values in the sent heartbeat information, if any exception occurs, the device displays the error message. |
| Remove all existing MDM profiles before proceeding else enrollment will fail. | While enrolling the device retains the MDM profile of the previous enrollment. In this scenario, the system displays the error message if the MDM profile does not exist. |
| This user neither have a valid admin initiated request nor Device Initiated is enabled, Thus the request cannot be processed. | During the device enrollment the device user does not have any valid enrollment request as Admin initiated or Device initiated . In this scenario, the user device enrollment request is null, so the device displays the error message. |
| Reset your password from the console. | <p>Scenario: The error message occurs, while authenticating a user with the given username and password:</p> <ul style="list-style-type: none"> - The user credentials are expired due to a policy defined by the EMM admin. <p>Thus, when a user tries to login, the user password reset flag settings are checked. If the password has expired, the device invalidates the session and ask the user to reset a new password from console.</p> |

| Store Messages | Scenarios |
|---|---|
| Enrollment has failed. You are not permitted to enroll without accepting the Terms and Conditions | During a device enrollment, a user denies to accept the Terms and Condition set by the EMM admin. Thus, the device enrollment is not complete and the device displays the error message. |
| Invalid username or password | The system authenticates a user with the given username and password. If the user credentials are invalid, the device displays the error message. |
| The user-agent is not supported | While downloading the Enterprise Store, if the received platform name is NULL for the User-Agent , the device displays the error message. |
| The User credentials have expired | The system authenticates a user with the given username and password. If the user credentials are expired due to some policy defined by the EMM admin, the device displays the error message. |
| Your account has been deactivated by EMM Admin. You will be logged out. | The error message is sent to all enrolled devices with a user in the following circumstances: - The device user is deactivated by EMM admin. The system performs the Enterprise Wipe action to all user devices and the user is immediately logged out from the Enterprise Store. |
| The User has exceeded the maximum limit allowed to enroll the devices. Try with another user | The EMM admin has set the number of device limit per user to enroll with EMM in the Application Settings > Usage settings page. If the user has reached the limit and further tries the next enrollment, the device displays the error message. |

| Store Messages | Scenarios |
|--|---|
| Existing Password does not match with the user | A user tries to reset the user password from the device. If the existing password does not match with the old password, the device displays the error message. |
| The User is deactivated. | The EMM admin has defined settings for the failed password attempts. The User is Locked/Disabled because of the failed login attempts. In this scenario, when a user tries to download the Enterprise Store or enroll with the EMM server, the device displays the error message. |
| The User is inactive | The User active flag in the database is inactive. When the user tries to enroll with the EMM server or tries to download the Enterprise Store, the device displays the error message. |
| Reset password is applicable only to LOCAL users | The Reset password for the user is requested and this pertains to a non-Local user such as AD user or any Identity user. In this scenario, the device displays the error message. Note: This option is hidden from the Launchpad but can be accessed through the REST client. |
| Enrollment Failed. The user is not authorized to enroll. | The user named as User_One is not added in the Enrollment AD group defined by the EMM admin. Thus, when User_One tries to enrol with the EMM server, the device displays the error message. |
| User Not Unique | The error message is displayed in the following scenarios: - While authenticating to the EMM server for downloading the Enterprise Store or - While login to the Enterprise store. - In both the circumstances, if the user id is not unique, the device displays the error message. The error message states to select the specific source to authenticate the user because the same user id is available from different sources in the EMM server. |

| Store Messages | Scenarios |
|--|---|
| A Password cannot be accepted with only spaces | While resetting the user password from a device, if a user has entered the blank password or only white spaces as a new password, the device displays the error message. |
| Workplace enrollment is not allowed for this user. Contact your administrator. | On Windows platform, a user tries to enrol the device in MAM mode from the device workplace. As workplace enrollment is allowed only for the MDM mode user, the device displays the error message. |
| You are not registered with this device | A user tries to login to Launchpad in EMM mode. The EMM admin checks the device enrollment through a Kony device id. If the system finds that the device is already enrolled with a different user, the device displays the error message. |
| Authorization failed. This device is not registered with you. Contact your EMM Admin for more information. | A user tries to login to Launchpad in MAM mode. The EMM admin checks the device enrollment through Kony device id. If the system finds that the device is already enrolled with a different user, the device displays the error message. |

| Store Messages | Scenarios |
|---|--|
| <p>Device Enrollment Successful. Enterprise Store installation is triggered and may take some time. Once it is installed, login into Enterprise Store using your credentials.</p> | <p>A user enrolls any Windows phone 8 device and the enrollment is successful. In this scenario, the device displays the information message with a device code to login to the Launchpad.</p> |
| <p>Device Enrollment Successful. For full EMM functionality, please inform your Administrator to update the Enterprise Certificate.</p> | <p>The EMM admin does not upload the certs for the Windows platform and a user enrolls any Windows device in No-certificate mode. In this scenario, the device displays the information message.</p> |

| Store Messages | Scenarios |
|---|---|
| <p>Device Enrollment successful. Enterprise Store installation is triggered and may take some time. Once it is installed, login into Enterprise Store using your credentials and provide the device code as {arg0}.</p> | <p>A user enrolls any Windows phone 8 device and the enrollment is successful. In this scenario, the device displays the information message with a device code to login to the Launchpad.</p> |
| <p>It is observed that you have unenrolled and enrolled back with a different userID. This operation is not supported. Unenroll and enroll back with earlier userID or contact admin</p> | <p>A user enrolls the same device with EMM after the un-enrolling with a different user ID. The system detects that the device ID is already enrolled with a different user. In this scenario, the device displays the error message.</p> |

| Store Messages | Scenarios |
|---|--|
| <p>Your access to corporate resources is suspended. Contact your administrator in case of any further queries.</p> | <p>The EMM admin performs an Enterprise wipe with suspended action for the enrolled Windows devices to restrict the user from accessing the Enterprise Store. If the device is suspended by the Admin and the user tries to login to the Launchpad, the device displays the error message.</p> |
| <p>It is observed that Future Enrollment is denied for this Device,thus Un-enroll has been initiated, Contact your admin.</p> | <p>The admin performs an Enterprise wipe with option as Allow Future Enrollemnet as No to add the device in future Enrollemnet Denied list. If the user tries to enroll the Windows devices, the device displays the error message.</p> |
| <p>Enter a device code.</p> | <p>A user tries to login to the Enterprise Store on Windows phone 8 device. In this scenario, the device displays the error message asking the device user to put the device code while login.</p> |
| <p>Enter a different device code.</p> | <p>A user tries to login to the Enterprise Store on windows phone 8 device and use any wrong device code for login. In this scenario, the device displays the error message asking the device user to put the different device code.</p> |

15. Frequently Asked Questions

I canceled the installation of a child app. But I still see the installation status as installing. Why?

On iOS devices, Kony Enterprise Store app takes five minutes time to send the data logs to the server about status of user action (Install or Cancel) on installing a child app on the device to Kony Management Administrator console. If you have canceled the child app installation, you might still see the status of the install process as **Installing** on the enterprise store on the device. If you check the status after five minutes, the status will be refreshed and you will see an **Install** option.

How do I send a notification to all users (iOS and Android) as an Administrator?

You can send notifications to all devices enrolled in Kony Management suite by creating devices sets. Once you have a device set, you can send messages to all devices in that device set.

Important: You can only send messages to devices that are enrolled in EMM enrollment mode.

Note: For devices enrolled in MAM/MCM mode, you must send a bulk email through your email service.

- [Sending a message to all devices](#)
- [Sending a message to all iOS devices](#)
- [Sending a message to all Android devices](#)

For more information on sending push notifications and email messages, refer [Kony Management User Guide](#).

15.1 Sending a Message to All Devices

To send a message to all devices, do the following:

1. In Kony Management admin console, under **Device Management**, click **Device Sets**. The Device Sets page opens with the list of existing device sets. By default, an All Devices set exists.

Device Sets [State / Status Help](#)


Displaying 1 - 4 of 4 - Display 10

| Device Set Name ▼ | State | Status | Last Updated On | Last Successful Publish | Actions | Permission Sets |
|------------------------|----------|-------------|---------------------------|---------------------------|-----------------|-----------------|
| Search Device Set Name | All ▼ | All ▼ | All ▼ | All ▼ | | |
| All Devices | Active ▼ | Published ▼ | 03 Jul, 2017 03:12:39 EDT | 03 Jul, 2017 03:12:39 EDT | Select Action ▼ | |
| Corporate Owned | Active ▼ | Published ▼ | 03 Jul, 2017 03:12:39 EDT | 03 Jul, 2017 03:12:39 EDT | Select Action ▼ | |
| Employee Owned | Active ▼ | Published ▼ | 03 Jul, 2017 03:12:39 EDT | 03 Jul, 2017 03:12:39 EDT | Select Action ▼ | |
| Shared | Active ▼ | Published ▼ | 03 Jul, 2017 03:12:39 EDT | 03 Jul, 2017 03:12:39 EDT | Select Action ▼ | |

Previous **Page (1/1)** Next

2. Click **All Devices**. The All Devices set details page opens with the Description tab open by default.

Device Set Details
[Device Sets](#) > [All Devices](#)



All Devices
 Created Date: 03 Jul, 2017 03:12:39 EDT
 Created By: admin

Device Set State : Active ▼

Device Set Status : Published ▼

Device Policy : Assign Policies

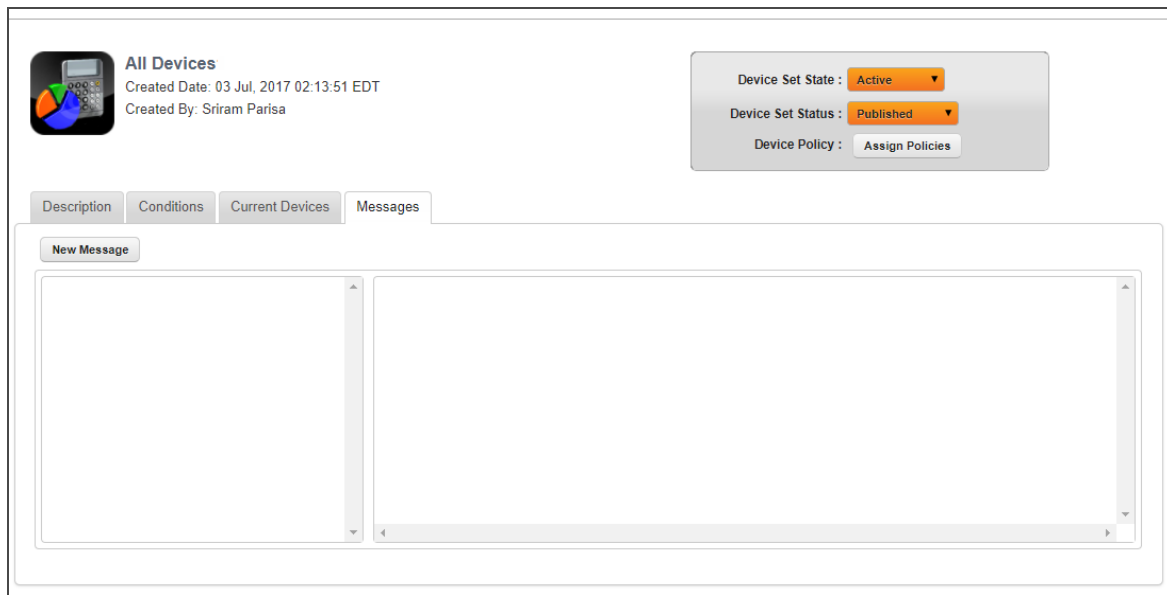
Description Conditions Current Devices Messages

Device Set Description

All Enrolled and Active Devices

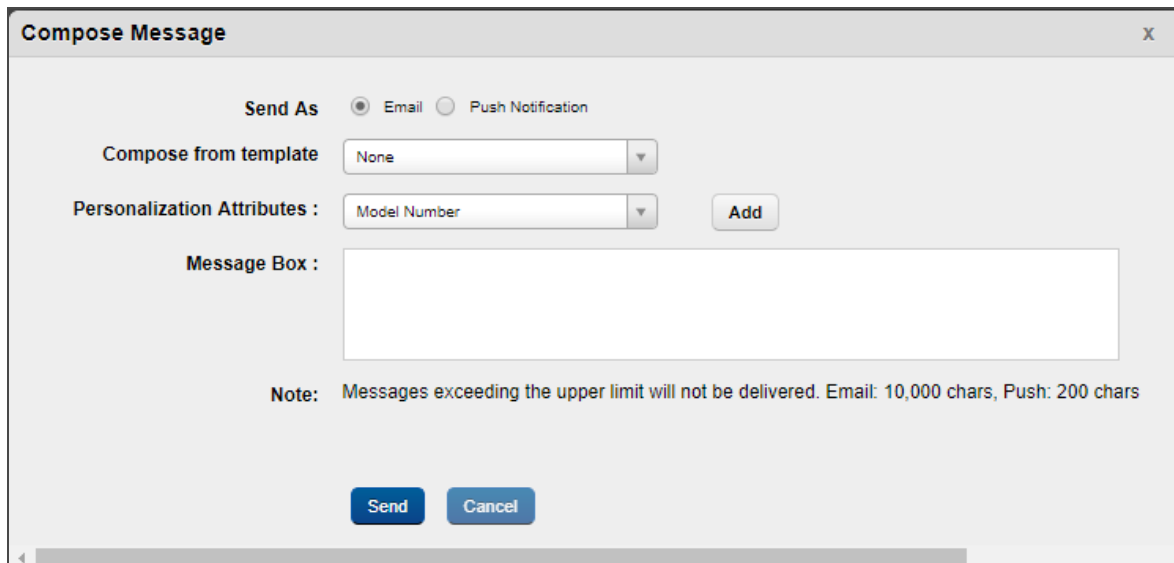
You have 450 characters left

3. Click **Messages**. The Messages tab opens.



The screenshot shows the 'Messages' tab for a device set named 'All Devices'. The device set is created on 03 Jul, 2017 02:13:51 EDT by Sriram Parisa. The 'Device Set State' is 'Active', the 'Device Set Status' is 'Published', and the 'Device Policy' is 'Assign Policies'. Below this information are four tabs: 'Description', 'Conditions', 'Current Devices', and 'Messages'. The 'Messages' tab is active, showing a 'New Message' button and a large empty text area for composing a message.

4. Click **New Message**. The Compose Message page appears.



The 'Compose Message' dialog box is shown. It has a title bar with 'Compose Message' and a close button. The 'Send As' field has radio buttons for 'Email' (selected) and 'Push Notification'. The 'Compose from template' field is set to 'None'. The 'Personalization Attributes' field is set to 'Model Number', with an 'Add' button next to it. The 'Message Box' is a large empty text area. A note at the bottom states: 'Note: Messages exceeding the upper limit will not be delivered. Email: 10,000 chars, Push: 200 chars'. At the bottom are 'Send' and 'Cancel' buttons.

5. In the **Send As** field, select **Push Notification**.
6. In the **Message Box**, enter your message.
7. Click **Send**. The Send Message - Success message appears.
8. Click **OK**. Your message is sent to all devices in the device set.

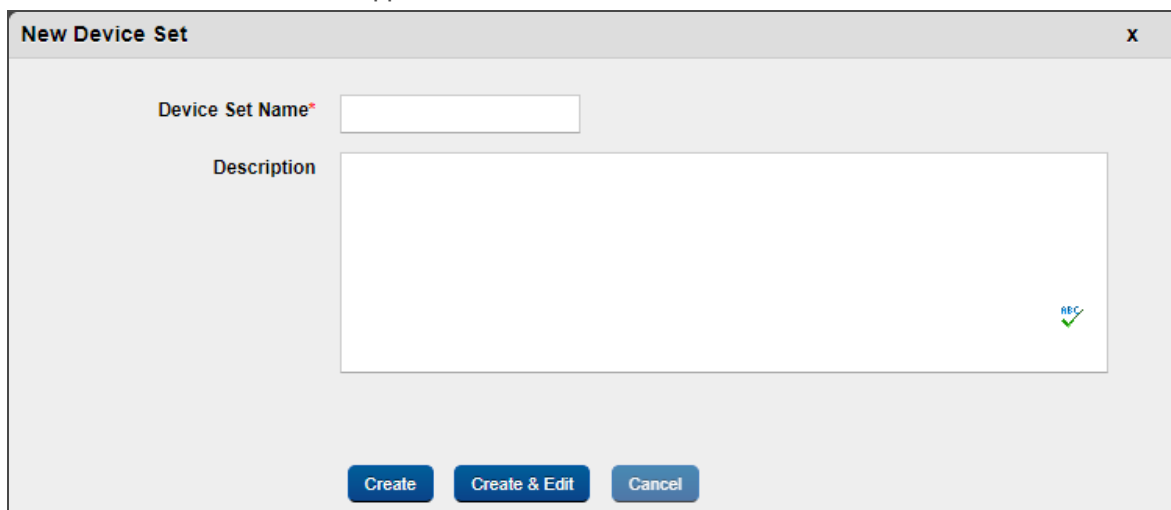
15.2 Sending a Message to all iOS devices

To create a new device set for iOS and send a message to all iOS devices, do the following:

1. In Kony Management admin console, under **Device Management**, click **Device Sets**. The Device Sets page opens with the list of existing device sets.
2. Click **+ New Device Set** next to the **Device Sets** label at the top of the page.



The **New Device Set** window appears.

A screenshot of a 'New Device Set' dialog box. The dialog has a title bar with 'New Device Set' on the left and a close button 'x' on the right. Inside the dialog, there are two input fields: 'Device Set Name*' with a small text box, and 'Description' with a larger text area. A small green checkmark icon with the text 'REC' is visible in the bottom right corner of the description area. At the bottom of the dialog, there are three buttons: 'Create', 'Create & Edit', and 'Cancel'.

3. In the **Device Set Name** field, enter **iOS Devices**.
4. In the **Description** field, enter a brief description for the device set.

- Click **Create & Edit**. The Device Set Details page opens with the Description tab open by default.

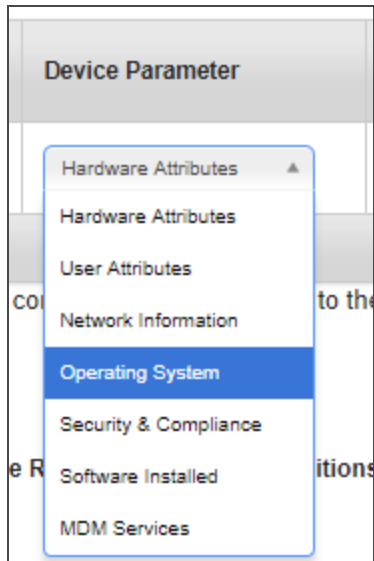
The screenshot shows the 'Device Set Details' page for a device set named 'iOS Devices'. The breadcrumb trail is 'Device Sets > iOS Devices'. The device set icon is a smartphone with a pie chart. The details include: 'Created Date: 03 Jul, 2017 22:50:59 EDT' and 'Created By: Sriram Parisa'. On the right, there are three controls: 'Device Set State' set to 'Draft', 'Device Set Status' set to 'Unpublished', and a button for 'Device Policy' labeled 'Assign Policies'. Below these are four tabs: 'Description' (selected), 'Conditions', 'Current Devices', and 'Messages'. The 'Description' tab contains a text area with the text 'All iOS Devices' and a character count 'You have 485 characters left'. At the bottom are three buttons: 'Save & Activate', 'Save & Continue', and 'Cancel'.

- Click **Conditions** tab. The Conditions tab opens.

The screenshot shows the 'Device Set Conditions' tab. It features a table with the following columns: 'Condition Number', 'Device Parameter', 'Device Attribute', 'Condition', 'Definition', and 'Add / Remove'. There is one row with the following data: Condition Number '1', Device Parameter 'Hardware Attributes', Device Attribute 'Device Model', Condition 'Contains', and an empty Definition field. The 'Add / Remove' column contains 'Add' and 'Remove' buttons. Below the table is a note: 'Click on the condition number to add it to the rules to build the Device Set.'

| Condition Number | Device Parameter | Device Attribute | Condition | Definition | Add / Remove |
|------------------|---------------------|------------------|-----------|------------|--------------|
| 1 | Hardware Attributes | Device Model | Contains | | Add Remove |

- From the **Device Parameter** list, select **Operating System**.

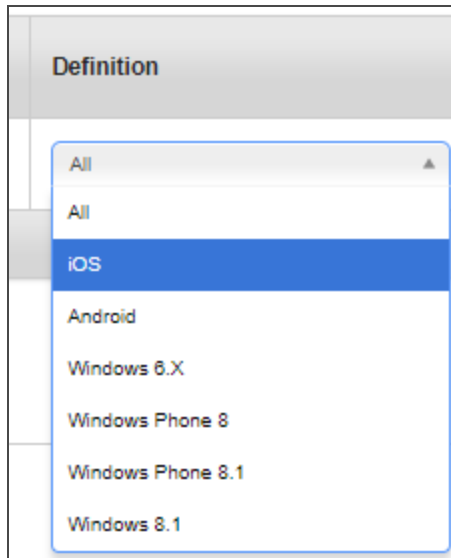


- From the **Device Attribute** list, select **Platform**.



- Leave the **Condition** list as is to **Equal To**.

- From the **Definition** list, select **iOS**.



The condition is added.

| Device Set Conditions | | | | | |
|-----------------------|------------------|------------------|-----------|------------|--|
| Condition Number | Device Parameter | Device Attribute | Condition | Definition | Add / Remove |
| 1 | Operating System | Platform | Equal To | All | <input type="button" value="Add"/> <input type="button" value="Remove"/> |

Click on the condition number to add it to the rules to build the Device Set.

- Click the Condition number to add it to the Definition set.
- Click **Validate & Search**. All devices that meet the definition criteria set will appear below.
- Click **Save & Activate**. The device set page appears with the newly created device set in the list. Note that the state of the device set is set to **Active**.

14. From the **Status** column of the device set, click **Published** to publish the device set.

| Device Set Name ▼ | State | Status |
|---|----------|----------------------------|
| <input type="text" value="Search Device Set Name"/> | All ▼ | All ▼ |
| iOS Devices | Active ▼ | Unpublished ▼ |
| All Devices | Active ▼ | Published ▼ Published ▼ |
| Corporate Owned | Active ▼ | Published ▼ |
| Employee Owned | Active ▼ | Published ▼ |
| Shared | Active ▼ | Published ▼ |

The Status Change dialog appears.

15. Click **Published** to publish the device set. The Status Change dialog appears.

Status Change x

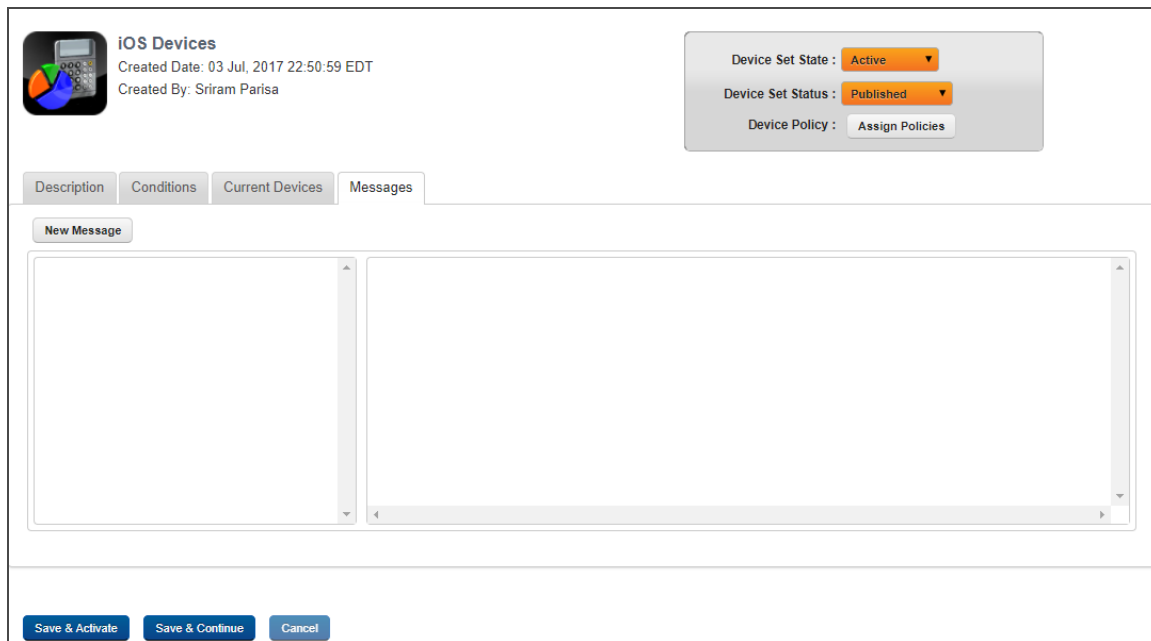
Comments

REC ✓

You have 473 characters left

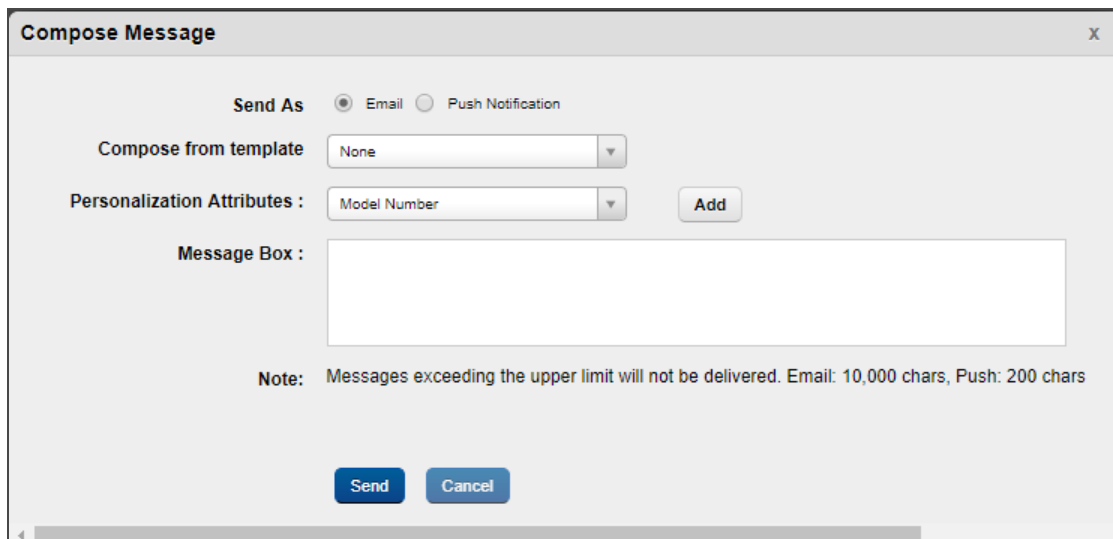
16. Enter your comments in the page and click **Publish**. A status change message appears.
17. Click **OK**.
18. Click the device set. The Device Set Details page appears.

19. Click **Messages**. The Messages tab opens.



The screenshot shows the 'Messages' tab for a device set named 'iOS Devices'. The device set was created on 03 Jul, 2017 22:50:59 EDT by Sriram Parisa. The 'Device Set State' is 'Active', the 'Device Set Status' is 'Published', and the 'Device Policy' is 'Assign Policies'. The 'Messages' tab is selected, and a 'New Message' button is visible. Below the button are two large text input fields for composing a message. At the bottom, there are three buttons: 'Save & Activate', 'Save & Continue', and 'Cancel'.

20. Click **New Message**. The Compose Message page appears.



The screenshot shows the 'Compose Message' dialog box. It has a title bar with 'Compose Message' and a close button 'X'. The 'Send As' field has radio buttons for 'Email' (selected) and 'Push Notification'. The 'Compose from template' field is set to 'None'. The 'Personalization Attributes' field is set to 'Model Number', with an 'Add' button next to it. The 'Message Box' is a large text input field. Below the message box, a note states: 'Note: Messages exceeding the upper limit will not be delivered. Email: 10,000 chars, Push: 200 chars'. At the bottom, there are 'Send' and 'Cancel' buttons.

21. In the **Send As** field, select **Push Notification**.
22. In the **Message Box**, enter your message.
23. Click **Send**. The Send Message - Success message appears.
24. Click **OK**. Your message is sent to all devices in the device set.

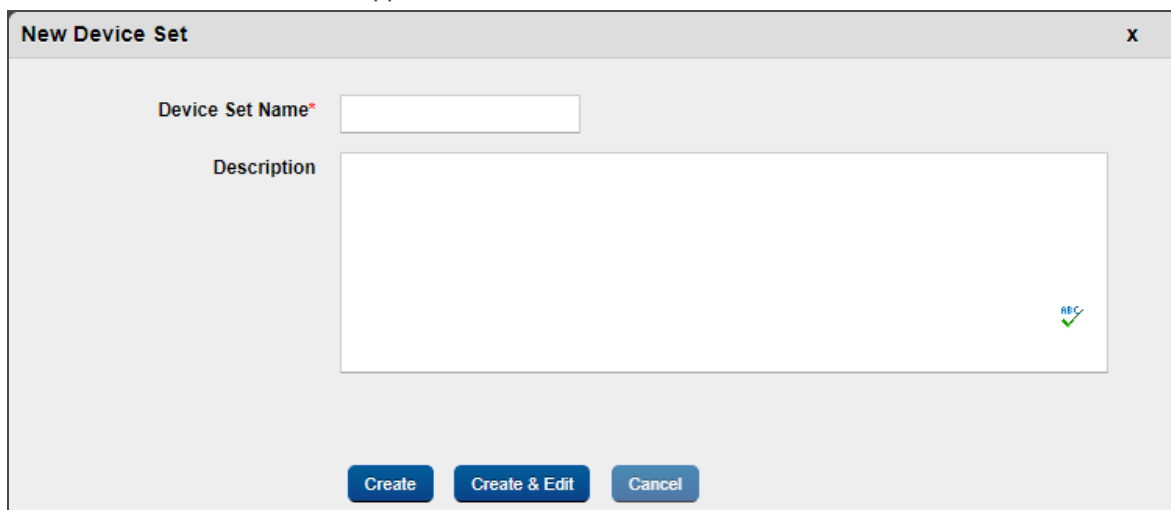
15.3 Sending a Message to all Android devices

To create a new device set for Android OS and send a message to all Android devices, do the following:

1. In Kony Management admin console, under **Device Management**, click **Device Sets**. The Device Sets page opens with the list of existing device sets.
2. Click **+ New Device Set** next to the **Device Sets** label at the top of the page.



The **New Device Set** window appears.


A screenshot of a modal dialog box titled 'New Device Set' with a close button (X) in the top right corner. The dialog has a light gray background. It contains two input fields: 'Device Set Name*' with a small asterisk and a white text box, and 'Description' with a larger white text area. At the bottom of the dialog are three blue buttons with white text: 'Create', 'Create & Edit', and 'Cancel'. A small green checkmark icon is visible in the bottom right corner of the description text area.

3. In the **Device Set Name** field, enter **Android Devices**.
4. In the Description field, enter a brief description for the device set.

5. Click **Create & Edit**. The Device Set Details page opens with the Description tab open by default.

Device Set Details

[Device Sets](#) > Android Devices



Android Devices
Created Date: 03 Jul, 2017 23:04:11 EDT
Created By: Sriram Parisa

Device Set State : Draft ▼

Device Set Status : Unpublished ▼

Device Policy : Assign Policies

Description Conditions Current Devices Messages

Device Set Description

All Android Devices

You have 481 characters left

Save & Activate
Save & Continue
Cancel

6. Click **Conditions** tab. The Conditions tab opens.

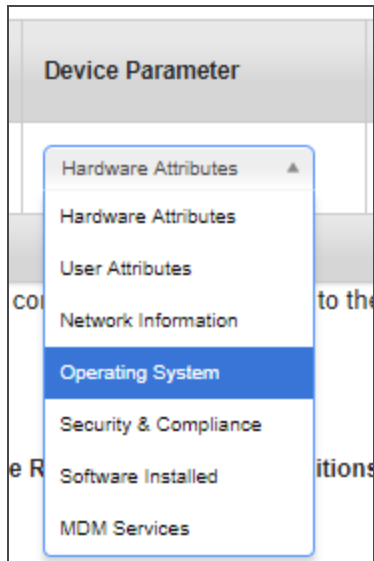
Description **Conditions** Current Devices Messages

Device Set Conditions

| Condition Number | Device Parameter | Device Attribute | Condition | Definition | Add / Remove |
|------------------|-----------------------|------------------|------------|---|--|
| 1 | Hardware Attributes ▼ | Device Model ▼ | Contains ▼ | <input style="width: 100%;" type="text"/> | Add Remove |

Click on the condition number to add it to the rules to build the Device Set.

- From the **Device Parameter** list, select **Operating System**.

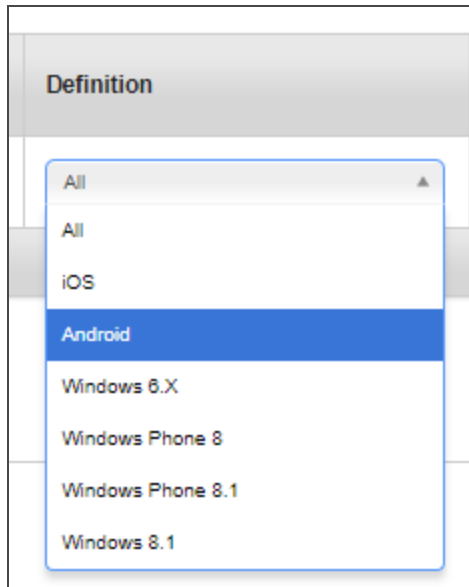


- From the **Device Attribute** list, select **Platform**.



- Leave the **Condition** list as is to **Equal To**.

- From the **Definition** list, select **Android**.



The condition is added.

- Click the Condition number to add it to the Definition set.
- Click **Validate & Search**. All devices that meet the definition criteria set will appear below.
- Click **Save & Activate**. The device set page appears with the newly created device set in the list. Note that the state of the device set is set to **Active**.

14. From the **Status** column of the device set, click **Published** to publish the device set.

| Device Set Name ▼ | State | Status |
|---|----------|----------------------------|
| <input type="text" value="Search Device Set Name"/> | All ▼ | All ▼ |
| Android Devices | Active ▼ | Unpublished ▼ |
| iOS Devices | Active ▼ | Published Unpublished ▼ |
| All Devices | Active ▼ | Published ▼ |
| Corporate Owned | Active ▼ | Published ▼ |
| Employee Owned | Active ▼ | Published ▼ |
| Shared | Active ▼ | Published ▼ |

The Status Change dialog appears.

Status Change x

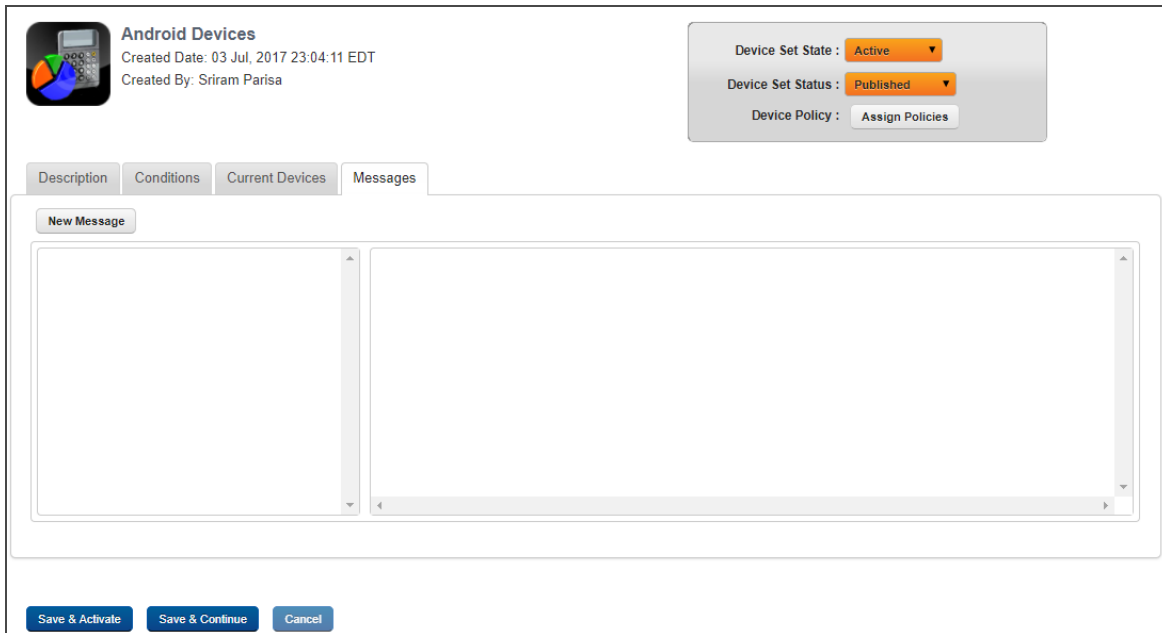
Comments

REC ✓

You have 473 characters left

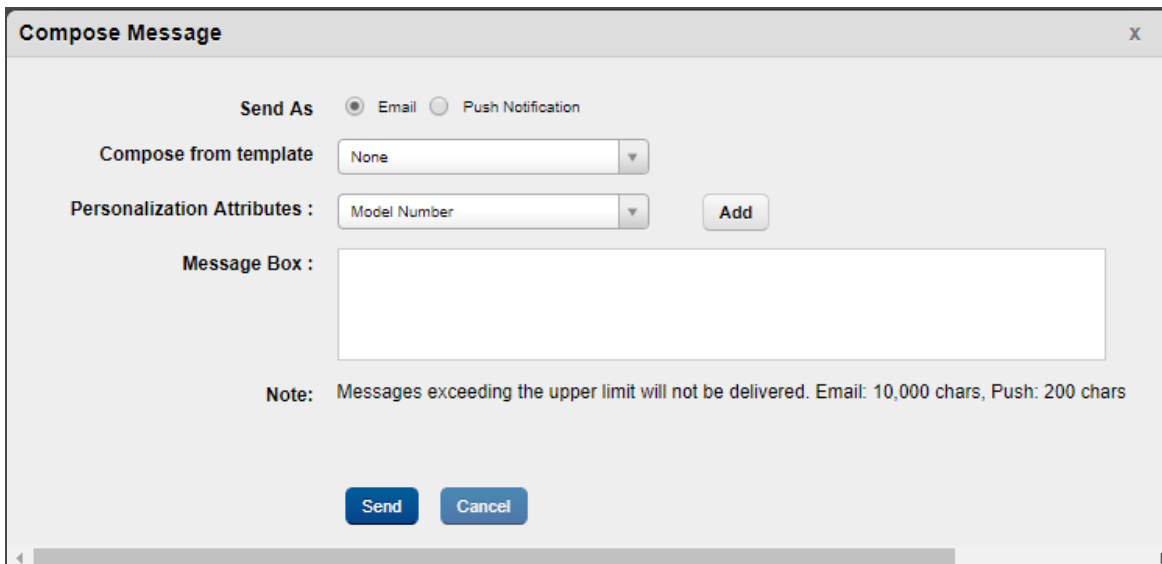
15. Enter your comments in it and click **Publish**. A status change message appears.
16. Click **OK**.
17. Click the device set. The Device Set Details page appears.

18. Click **Messages**. The Messages tab opens.



The screenshot shows the 'Android Devices' configuration page. At the top left, there is a device icon and the text 'Android Devices', 'Created Date: 03 Jul, 2017 23:04:11 EDT', and 'Created By: Sriram Parisa'. On the top right, there are three dropdown menus: 'Device Set State' set to 'Active', 'Device Set Status' set to 'Published', and 'Device Policy' with an 'Assign Policies' button. Below these are four tabs: 'Description', 'Conditions', 'Current Devices', and 'Messages'. The 'Messages' tab is active, showing a 'New Message' button and a large empty text area for composing a message. At the bottom, there are three buttons: 'Save & Activate', 'Save & Continue', and 'Cancel'.

19. Click **New Message**. The Compose Message page appears.



The screenshot shows the 'Compose Message' dialog box. It has a title bar with 'Compose Message' and a close button 'X'. Inside, there are two radio buttons for 'Send As': 'Email' (selected) and 'Push Notification'. Below that is a 'Compose from template' dropdown menu set to 'None'. There is a 'Personalization Attributes' section with a dropdown menu set to 'Model Number' and an 'Add' button. A large 'Message Box' text area is provided for entering the message. At the bottom, there is a 'Note' stating: 'Messages exceeding the upper limit will not be delivered. Email: 10,000 chars, Push: 200 chars'. At the very bottom are 'Send' and 'Cancel' buttons.

20. In the **Send As** field, select **Push Notification**.
21. In the **Message Box**, enter your message.
22. Click **Send**. The Send Message - Success message appears.
23. Click **OK**. Your message is sent to all devices in the device set.

What are the scenarios in which Kony Management triggers wrapping of Enterprise Stores and Enterprise Apps?

Note: When there is a major release or hot fix deployed on Kony Management cloud, cloud deployment will take care of wrapping and creating a new version of the enterprise store as and if required.

Branding

Kony Management provides a default Branding set that can be used for an enterprise store for branding. When a new branding set is created or if an existing branding set is modified, when the new/modified set is applied on an enterprise store, the store is re-wrapped.

Specifically:

- Any change in the configuration of a Branding set which is assigned to an Enterprise Store will trigger wrapping for that Enterprise Store.
- Also, if a Branding set assigned for an Enterprise Store is changed to another Branding set, wrapping would trigger for that Enterprise store.

Application Settings - Certificates:

Modifications to any certificates in the Application settings triggers wrapping of enterprise apps and enterprise stores associated with those certificates.

- Android Key Store / Android Maps / Project ID - All Android and Android Tablet Platform Enterprise Stores and Enterprise Apps.
- IOS Enterprise Distribution Certificate - All iOS Enterprise Stores and Apps.
- IOS Wild Card Provisioning Profile - All iOS Enterprise Apps.
- IOS Enterprise Store Provisioning Profile - All iOS Enterprise Stores.
- Two-Way SSL Certificate - Android and Android Tablet and iOS Enterprise Stores would be re-wrapped.

Application Settings - Encryption Key:

Using the **Encryption Key** feature in the **Application settings** page, an administrator can generate new encryption keys or schedule an automated triggering of generating an encryption key.

When new encryption keys are generated, wrapping is triggered for enterprise stores and all “wrap and signed” enterprise apps would be triggered.

Note: Wrapping would be triggered for Android, Android Tablet and iPad and iPhone platforms.

Device Settings - Tracking Settings:

In the Device Settings page, when you modify the rule for the **Enable Device Location Tracking** feature, wrapping will be triggered.

Note: All Enterprise stores (All platforms) and Enterprise Apps (All platforms).

Authentication Settings - Kony Fabric Authentication settings:

In the Authentication Settings page, wrapping can be triggered in two scenarios.

- When you enable the Use Kony Fabric Identity feature, wrapping will be triggered for all Enterprise Stores (excluding windows platform).
- If the Use Kony Fabric Identity feature is already enabled, modifications to the following will trigger wrapping.
 - Change in the App Key/App Secret
 - Change to the Enable SSO feature
 - Android and Android Tablet - when Android Broadcast phrase is modified.
 - iPad and iPhone - when iOS Keychain group is modified.

Security

- User name and password are stored in the device in encrypted form.
- Sensitive information (for example, Password) is masked when it is displayed on the screen.
- Sensitive data (for example, Password) is cleared from the forms when navigating away from the forms.
- All sensitive information is encrypted using industry standard SSL during access and transmission between client and server.
- Copy and Paste function is disabled for sensitive data (for example, Password).

Logging

- Sensitive data such as user name and password are not logged to the console or files (server/client side). Where required, the sensitive data is encrypted and moved into logs.
- Sensitive information like session IDs, user names are not printed in the logs.

App Sign In

- When you sign into the application the first time, you must be connected to the internet so that the application data and the latest version of the metadata around the application screens are fetched from the backend
- The application data and metadata are saved on the device. Each time a user performs a manual sync, the latest data is saved on the device.
- If a new user signs into the same device and from the same application, the previous user's data is removed from the device and the new user's data is saved.
- On subsequent log-in attempts:
 - If a user is online, the user credentials are validated against the backend.
 - If a user is offline, the user credentials are validated against the credentials stored in the device, and the last retrieved data and forms are displayed in the application.

Session Management

- Session is created when a user signs in with valid credentials.
- Session also gets terminated if the application is force-closed.
- User session details are cleared from both device and server, when the session is terminated.

Error Handling

- Validation alerts are displayed for each field or rule (no consolidation).
- The app throws appropriate errors during device interrupts. For example, receive a call while in the middle of a session.

Performance and Memory Requirements

- Throughout the application, a user is shown a busy indicator with blocked page UI implemented as long

as the processing is in progress.

Wrapping/Signing Requirements

- An administrator can configure wrapping server even after installation.
 - iOS: By modifying the hosts.properties file.
 - Windows: hosts_win.properties file.
 - Android: Same as the Android SDK ssetup on the installation computer.

Configuring four Apple Mac server

- An administrator must configure four Apple MAC servers for fail-safe.

What should I do when my Apple WWDR certificate expires?

When Apple WWDR certificate expires, it impacts the Enterprise Distribution certificate. To continue to use it to sign apps, you must delete the old WWDR from the keychain on the signing Mac system. Please follow the steps given below:

1. Open Keychain access on the mac system.
2. Enable **View>Show Expired Certificates**.
3. Go to System Keychain and delete the expired WWDR certificate
4. Follow step number three for Login Keychain.
5. Import the new WWDR certificate into keychain.

What is the recommended way to install the downloaded Kony Management Enterprise Store apk on my Android device.

- After you download the Kony Management Enterprise Store apk using any web browser, navigate to your **Downloads** folder on your android device.
- You can also use a file manager application to open the Kony Management Enterprise Store apk. The apk can be found on the Device storage in the **Download** folder. Using any file manager application freely available on the Google playstore, you can access the Download folder. Clicking the Kony Enterprise

Store from the Download folder will install the Kony Management Enterprise Store app on your device.

I am an administrator and a user contacted me that he got an error message **Cannot login on the device**, please contact your administrator.

The user's device might be a rooted or jailbroken device. If your Device Settings is set to not allow rooted or jailbroken device, the user will not be able to log in through the enterprise store. In your device settings, if you have configured it to not allow jailbroken or rooted devices,

For iOS Devices

- Jailbroken devices will not be allowed to log in to the enterprise store. The user will receive a **Cannot login on the device, please contact your administrator** error message.

For Android devices

- **If the device is hard rooted:** Devices will not be allowed to log in to the enterprise store. The user will receive a **Cannot login on the device, please contact your administrator** error message.
- **If the device is soft rooted (malicious apps installed on the device):** Devices will not be allowed to log in to the enterprise store. The user will receive a **Cannot login on the device, please contact your administrator** error message. The user may have to uninstall any malicious apps and try logging in. In some cases a device reboot will be necessary after removing malicious apps before trying to login.

Android wrapping is failing after I upgraded from Java 7 to Java 8.

From V8 release, Kony Management does not support Java 7. If you upgraded from Java 7 to Java 8, Android wrapping may fail. If you encounter the following problem, see the solution available.

```
Exception in thread "main" brut.androlib.AndrolibException:
java.io.IOException: The system cannot find the path specified
at brut.androlib.Androlib.buildResourcesFull(Androlib.java:493)
at brut.androlib.Androlib.buildResources(Androlib.java:427)
at brut.androlib.Androlib.build(Androlib.java:326)
at brut.androlib.Androlib.build(Androlib.java:264)
at brut.apktool.Main.cmdBuild(Main.java:231)
at brut.apktool.Main.main(Main.java:84)
Caused by: java.io.IOException: The system cannot find the path specified
at java.io.WinNTFileSystem.createFileExclusively(Native Method)
```

```
at java.io.File.createTempFile(Unknown Source)
at java.io.File.createTempFile(Unknown Source)
at brut.androlib.Androlib.buildResourcesFull(Androlib.java:472)
```

To fix the wrapping fail problem, do the following:

1. Navigate to the catalina property file location. For example, `<EMM-InstalledDirectory>/tomcat/conf/`
2. Open the **catalina.properties** file with a note editor.
3. Add the following towards the end of the file.
`java.io.tmpdir=<temppath>`
Replace **<temppath>** with some folder name of your choice.
4. Verify that the %temp% path exists by running appropriate commands in your windows server machine.
5. Restart the Tomcat server.
6. Re-wrap your Android application. It should work fine.

16. Annexure

16.1 Internet Explorer 9 Compatibility Issues

Issue

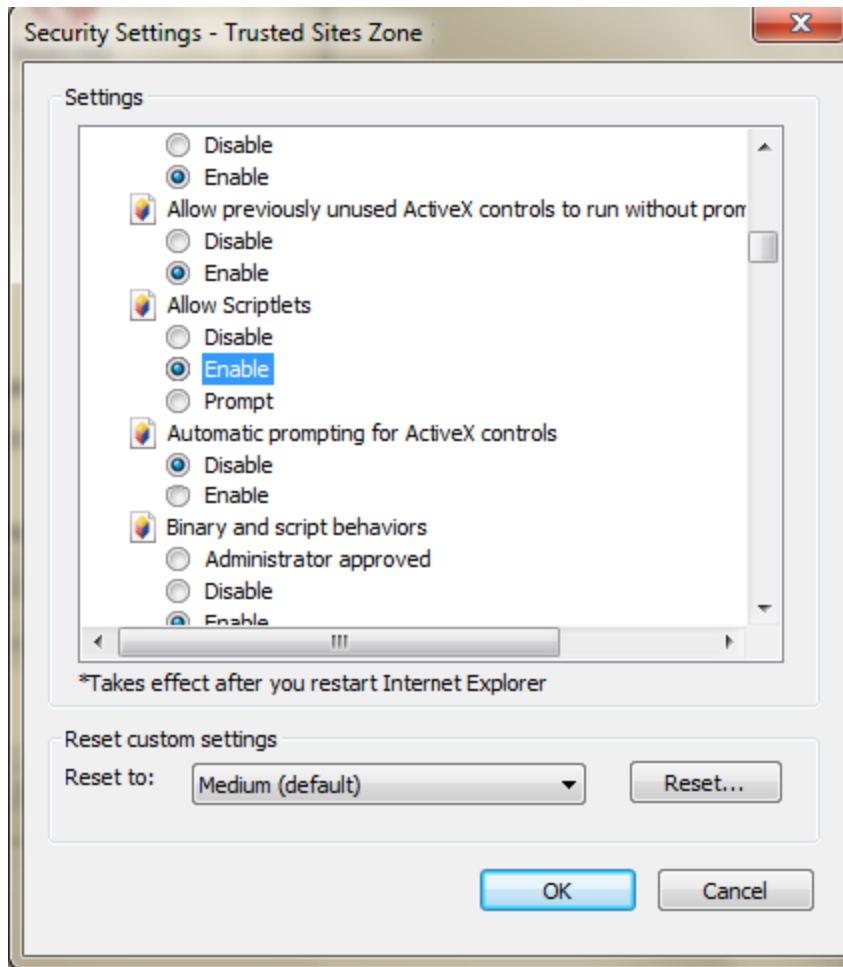
If you login to EMM application using Internet Explorer 9, and when you unpublish a policy from the Policy Details page, IE9 is unable to resolve the resultant page. To resolve this issue, follow the below workaround.

If you have issues with validation for Image size (it checks for the image size to be less than 65KB) in IE9, Admin should configure following the below workaround.

Workaround

To configure settings for Internet Explorer 9, follow these steps:

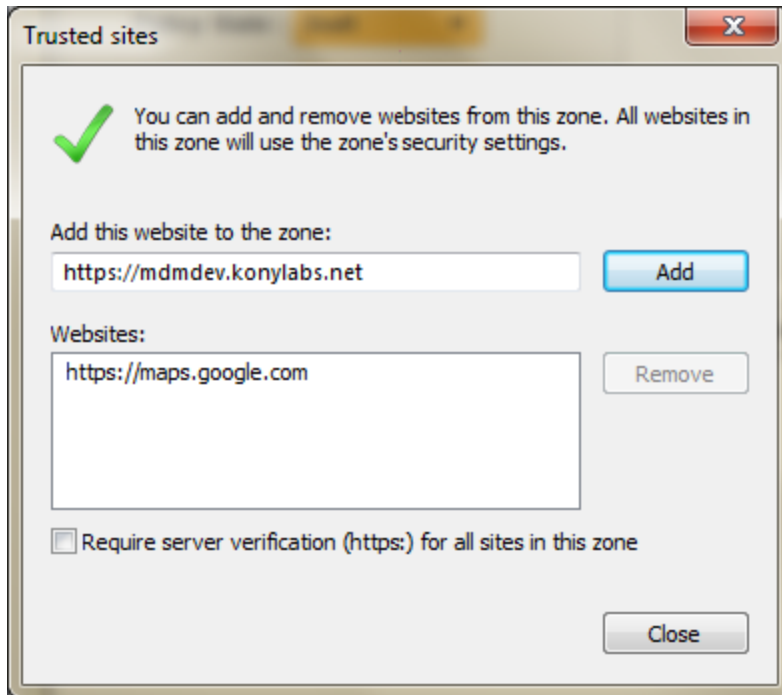
1. Go to Internet Option > Click Security tab > Select Custom Level to open Security settings in IE9 browser.



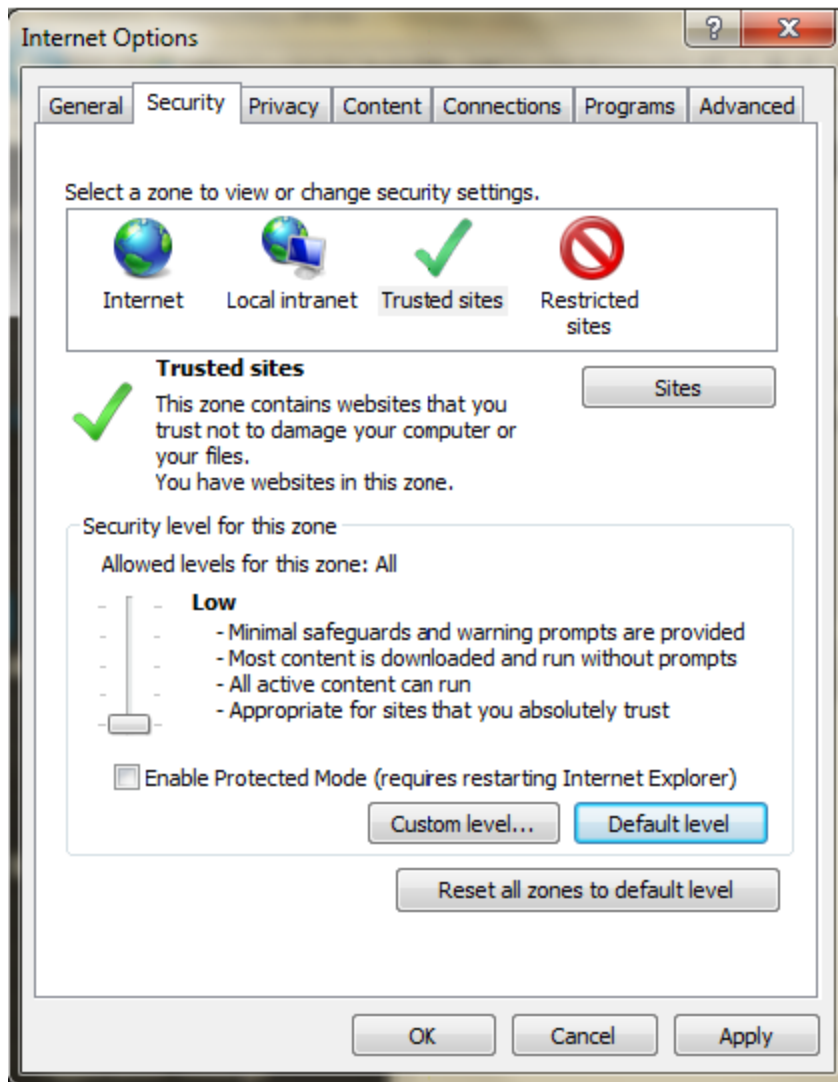
Pop-up appears.

2. In the popup go to ActiveX controls and Plug-ins and Enable Allow Scriptlets.
3. Go to Internet Option > Click Security tab > Select Sites to open Trusted Sites.

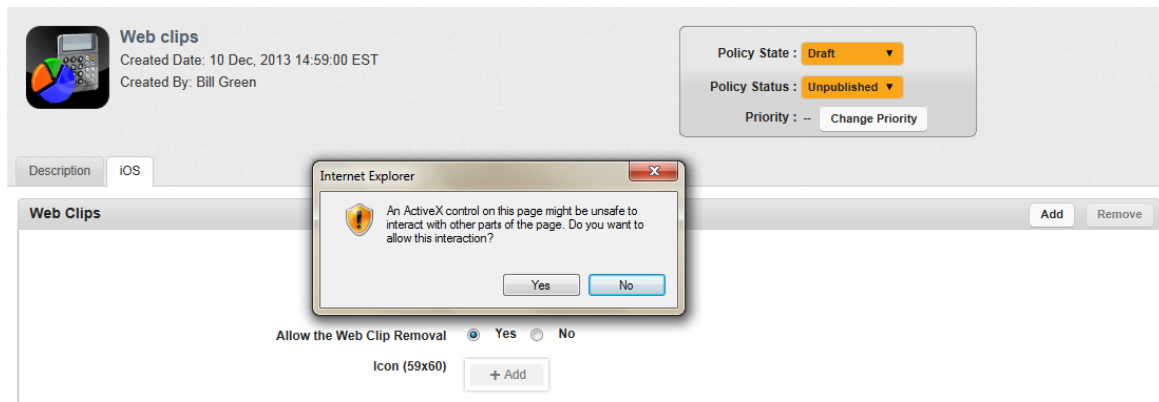
Trusted Sites Pop-up appears.



4. Ensure that current website is listed in the Websites list, else enter the URL in **Add this website to the zone** text field. Click the **Add** button.



5. Go to Internet Option>Click Security tab.and set the Security level Zone to **Low** by dragging the scroll bar. Click Apply to save the setting.



6. Once above steps are performed, refresh the page and go to Webclips policy. But, before selecting the file, the system prompts the ActiveX warning message. Click Yes to proceed,
7. After selecting the file, Webclips policy performs file validation and ensures the image size is less than 65 KB.